PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-101533
(43)Date of publication of application : 04.04.2003

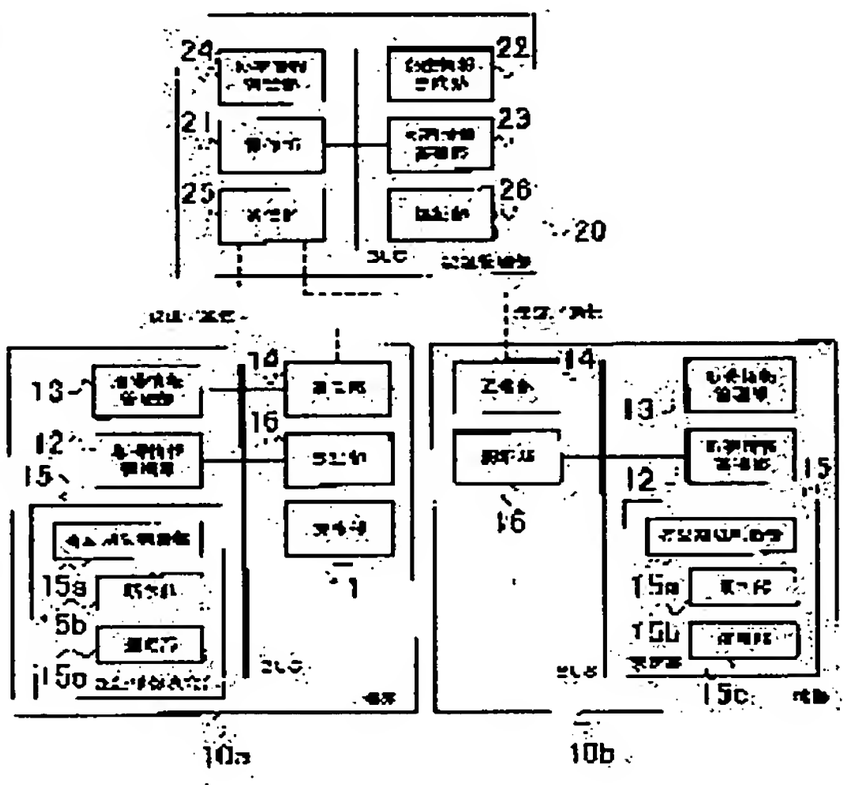
(51)Int.CI. H04L 9/32
G06F 15/00
H04L 9/08

(21)Application number : 2001-292581
(22)Date of filing : 25.09.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : YAMAGUCHI KENSAKU
NAKAKITA HIDEAKI
HASHIMOTO MIKIO

(54) DEVICE AUTHENTICATION MANAGEMENT SYSTEM AND METHOD THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent occurrence of a situation where each device cannot start communication with each other when there is a difference in the expiration time of the effective period for a common key used by each device in authentication among devices.
SOLUTION: A device authentication management system obtaining a predetermined secret information from a authentication management means manages the secret information, and conducts authentication for communication with other devices using the secret information. The authentication management means comprises a generation means for generating the secret information having a first authentication information for communication between the authentication management means and the device, and a second authentication information for communication between the device and other devices, a first authentication means for conducting authentication for communication with the device using the first authentication information generated by the generation means, and a first transmission means for transmitting the second authentication information, based on authentication by the first authentication means.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－101533
(P2003－101533A)
(43)公開日　平成15年４月４日(2003.4.4)

(51)Int.Cl.⁷	識別記号	FI	テーマコード（参考）
H04L 9/32		G06F 15/00	330C 5B085
G06F 15/00	330	H04L 9/00	675A 5J104
H04L 9/08			601B
			601E
			675D

審査請求　未請求　請求項の数11　ＯＬ　（全 29 頁）

(21)出願番号　特願2001－292581(P2001－292581)

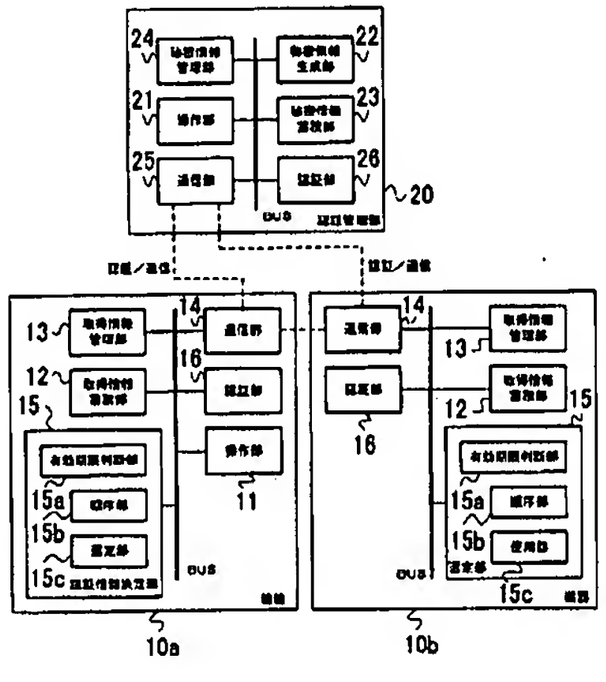
(22)出願日　平成13年９月25日(2001.9.25)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　山口　健作
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　中北　英明
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100083806
弁理士　三好　秀和　（外７名）

最終頁に続く

(54)【発明の名称】　機器認証管理システム及び機器認証管理方法

(57)【要約】
【課題】　各機器が、各機器との間の認証に用いる共通鍵の有効期限の終了時刻に差がある場合に、各機器間で行われる通信を開始することができなくなることを防止する。
【解決手段】　所定の秘密情報を管理する認証管理手段から前記秘密情報を取得した機器が、取得した該秘密情報を用いて他の機器との間で通信をするための認証を行う機器認証管理システムであって、前記認証管理手段が、前記認証管理手段と前記機器との間で通信を行うための第一認証情報と、前記機器と他の機器との間で通信を行うための第二認証情報とを有する前記秘密情報を生成する生成手段と、前記生成手段で生成された前記第一認証情報を用いて、前記機器との間で通信をするための認証を行う第一認証手段と、前記第一認証手段の認証に基づいて前記第二認証情報を送信する第一通信手段とを有することを特徴とするものである。



【特許請求の範囲】
【請求項１】　所定の秘密情報を管理する認証管理手段から前記秘密情報を取得した機器が、取得した該秘密情報を用いて他の機器との間で通信をするための認証を行う機器認証管理システムであって、
前記認証管理手段は、
前記認証管理手段と前記機器との間で通信を行うための第一認証情報と、前記機器と他の機器との間で通信を行うための第二認証情報とを有する前記秘密情報を生成する生成手段と、
前記生成手段で生成された前記第一認証情報を用いて、前記機器との間で通信をするための認証を行う第一認証手段と、
前記第一認証手段の認証に基づいて前記第二認証情報を送信する第一通信手段とを有し、
前記機器は、
前記認証管理手段から予め取得してある前記第一認証情報を用いて、前記第一認証手段との間で通信をするための認証を行う第二認証手段と、
前記第二認証部の認証に基づいて前記第一通信手段から前記第二認証情報を受信する第二通信手段とを有することを特徴とする機器認証管理システム。
【請求項２】　請求項１に記載の機器認証管理システムであって、
前記第二認証手段は、前記第二通信手段で受信した第二認証情報を用いて、前記他の機器との間で通信をするための認証を行う機能を有し、
前記第二通信手段は、前記第二認証手段の認証に基づいて、前記他の機器との間で通信を行う機能を有することを特徴とする機器認証管理システム。
【請求項３】　請求項１又は請求項２に記載の機器認証管理システムであって、
前記第二認証情報は、該第二認証情報を識別するための識別子と、前記第二認証情報を使用することができる有効期限情報とを有することを特徴とする機器認証管理システム。
【請求項４】　請求項３に記載の機器認証管理システムであって、前記機器は、
前記他の機器が有する複数の前記第二認証情報に含まれる前記識別子を取得し、その取得した前記識別子と、前記機器が有する複数の前記第二認証情報に含まれる前記識別子との間で共通する前記識別子を抽出して、その抽出した前記識別子に対応する前記第二認証情報のうち、該識別子に対応する前記有効期限情報に基づいて、該有効期限情報に対応する一つの前記第二認証情報を選定する第一選定手段と、
前記第二認証手段は、前記第一選定手段で選定された第二認証情報に基づいて、前記他の機器との間で通信をするための認証を行う機能を有することを特徴とする機器認証管理システム。
【請求項５】　請求項２又は請求項３に記載の機器認証管理システムであって、
前記第二通信手段が前記認証管理手段から前記第二認証情報を取得した時間を、前記第二認証情報に付加する時間付加手段と、
前記時間付加手段で前記時間が付加された前記第二認証情報を複数取得し、その前記時間が付加された複数ある前記第二認証情報の中から、付加された前記時間に基づいて、該時間に対応する一つの前記第二認証情報を選定する第二選定手段と、
前記第二認証手段は、前記第二選定手段で選定された前記第二認証情報に基づいて、前記他の機器との間で認証を行う機能を有することを特徴とする機器認証管理システム。
【請求項６】　請求項２に記載の機器認証管理システムであって
前記第二認証情報を所定の周期毎に生成する前記生成手段と、
前記生成手段で所定の周期毎に生成された前記第二認証情報を複数取得し、その複数取得した前記第二認証情報の個数が所定の個数を超えたときは、取得した複数ある前記第二認証情報のうちのいずれかを削除する第三選定手段とを有することを特徴とする機器認証管理システム。
【請求項７】　所定の認証情報を管理する認証管理手段から前記認証情報を取得した機器が、取得した該認証情報を用いて他の機器との間で通信をするための認証を行う機器認証管理方法であって、
前記認証管理手段は、
前記認証管理手段と前記機器との間で通信を行うための第一認証情報と、前記機器と他の機器との間で通信を行うための第二認証情報とを有する前記認証情報を生成するステップと、
生成された前記第一認証情報を用いて、前記機器との間で通信をするための認証を行うステップと、
前記機器との間で通信をするための認証に基づいて前記第二認証情報を送信するステップとを有し、
前記機器は、
前記認証管理手段から予め取得してある前記第一認証情報を用いて、前記認証管理手段との間で通信をするための認証を行うステップと、
前記認証管理手段との間で通信をするための認証に基づいて、前記認証管理手段から前記第二認証情報を受信するステップとを有することを特徴とする機器認証管理方法。
【請求項８】　請求項７に記載の機器認証管理方法であって、前記機器は、前記認証管理手段から受信した第二認証情報を用いて、前記他の機器との間で通信をするための認証を行うステップと、
前記他の機器との間で通信をするための認証に基づい

て、前記他の機器との間で通信を行うステップとを有することを特徴とする機器認証管理方法。

【請求項９】　請求項７又は請求項８に記載の機器認証管理方法であって、前記第二認証情報は、前記第二認証情報を識別するための識別子と、前記第二認証情報を使用することができる有効期限情報とを有することを特徴とする機器認証管理方法。

【請求項１０】　請求項９に記載の機器認証管理方法であって、前記機器は、

前記他の機器が有する複数の前記第二認証情報に含まれる前記識別子を取得し、その取得した前記識別子と、前記機器が有する複数の前記第二認証情報に含まれる前記識別子との間で共通する前記識別子を抽出して、その抽出した前記識別子に対応する前記第二認証情報のうち、該識別子に対応する前記有効期限情報に基づいて、該有効期限情報に対応する一つの前記第二認証情報を選定するステップと、

選定された前記第二認証情報に基づいて、前記他の機器との間で通信をするための認証を行うステップとを有することを特徴とする機器認証管理方法。

【請求項１１】　請求項８又は請求項９に記載の機器認証管理方法であって、前記機器は、

前記認証管理手段から前記第二認証情報を取得した時間を、前記第二認証情報に付加するステップと、

前記時間が付加された前記第二認証情報を複数取得し、その前記時間が付加された複数ある前記第二認証情報の中から、付加された前記時間に基づいて、該時間に対応する一つの前記第二認証情報を選定するステップと、

選定された前記第二認証情報に基づいて、前記他の機器との間で認証を行うステップとを有することを特徴とする機器認証管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、所定の秘密情報を管理する認証管理手段から前記秘密情報を取得した機器が、取得した秘密情報を用いて他の機器との間で通信をするための認証を行う機器認証管理システム及び機器認証管理方法に関する。

【０００２】

【従来の技術】近年のLAN(Local Area Network)技術の発達に伴い、オフィス環境では、PC(Personal Computer)間の接続を中心として、ネットワーク化が進行している。このような有線LANの普及の一方では、有線LANの一部分を無線で置換する無線LAN化も進んでいる。例えば、この無線LAN化によれば、有線LANに無線基地局を接続し、この基地局へ複数の携帯型パーソナルコンピュータを無線で接続することができる。

【０００３】そして、携帯型パーソナルコンピュータが、有線LANにイーサネット（登録商標）接続されているパーソナルコンピュータとの間で無線により通信接続を行い、その通信接続が行われたパーソナルコンピュータのファイルを編集することができる。これにより、携帯型パーソナルコンピュータは、有線LANへ無線アクセスを行っていることになる。

【０００４】また、基地局と携帯型パーソナルコンピュータの部分との間は、無線LANを形成していることにもなる。このような無線LANの利点は、伝送路として電波や赤外線などを利用するので配線敷設が不要なこと、ネットワークの新設やレイアウト変更が容易なことなどが挙げられる。

【０００５】無線LANの導入は、IEEE 802.11の標準化によって、拍車がかかっている。IEEE802.11では、1997年に2.4GHz帯の無線LAN仕様を、1999年に5GHz帯の無線LAN仕様を、それぞれ完成させている。2.4GHz帯の無線LAN仕様の伝送速度は、1～2Mbpsのものと11Mbpsのものとがあり、さらに20Mbpsを超える仕様が現在検討中である。最近、この2.4GHz帯の無線ＬＡＮ仕様に準拠した製品が、各社から発売されるようになり、基地局や無線PCカードが、普及価格帯に入りつつある。

【０００６】一方、5GHz帯の無線LAN仕様の伝送速度は、20～30Mbpsを実現できる。また、5GHz帯は、2.4GHz帯とは異なり、現在はほぼ未使用な通信周波数帯域で、かつ、より高速な伝送速度が容易に見込めるため、次世代の無線LAN仕様と期待されている。最近では、5GHz帯の通信機能を有するチップの価格が、1チップ35ドルで2001年中に発売予定というベンチャ企業も現れており、5GHz帯で行われる通信も身近になりつつある。

【０００７】更に、Bluetoothによる通信方式が、携帯電話業界や家電業界やPC業界を巻き込んで、あらゆる機器に搭載されようとしている。このBluetoothによる通信方式も2.4GHz帯の無線システムであるが、Bluetoothによる通信方式を採用したチップの価格は1チップ5ドル程度という低コストと、Bluetoothによる通信方式は幅広い業種の約2000社から賛同を得ていること、Bluetoothによる通信方式を用いた無線機器は製品化と直結した標準作成活動を行っていることなどから、Bluetoothによる通信方式を用いた無線機器は、世界的に普及すると見込まれている。

【０００８】以上のような状況から、無線機器が普及するに伴いこれらの技術の使用範囲は、オフィス環境だけでなく、一般家庭にも進んでいくものと考えられる。特に、家庭内において配線敷設が不要となる点は、オフィス環境の場合よりもさらに大きな利点である。

【０００９】しかし、無線による操作は容易な反面、無線機器間の接続は、ケーブル接続などの場合のように明示的な接続ではないという特徴から、セキュリティやプライバシの保護が問題となりやすい。無線機器は、家の外から、その無線機器が勝手にコントロールされることや、その無線機器から個人的な情報が盗まれることや、或いは、無線機器内にあるデータが壊されたりする可能

性がある。

【００１０】また、インターネットでの接続は、パートタイム接続から常時接続に移行しつつあるが、これに伴い無線ネットワークインタフェースで常時接続されることが一般的になると、第三者が、ファイアウォールを回避し、無線ネットワークインタフェースを経由して、パーソナルコンピュータに進入する可能性がある。

【００１１】更に、一般家庭ユーザは、盗聴やセキュリティに関連する脅威が必要であることを、コンピュータ業界のコンピュータウイルスに関連した報道やテレビ番組などで多少の知識を得られるような状況の中では、なんとなく不安を抱くものと想像される。

【００１２】ビジネス環境では、このような脅威に対して、専門家を雇うなどして対策を打つことが比較的容易であり、IPSECやファイヤウォールなどを実装して、かつ、これらのソフトウエアを継続して更新することが必要となるが、家庭環境では、このようなことは一般的に望みにくいものである。このため、家庭内で無線機器を使用する際には、外部から盗聴などをされないようにするためのセキュリティ管理を充実する必要がある。

【００１３】この家庭内でセキュリティ管理するには、先ず、各機器のセキュリティを統括的に管理する認証管理部を設置する。そして、認証管理部が各機器のセキュリティを行うには、セキュリティ管理を希望する各機器が認証管理部に登録を行う。この認証管理部にセキュリティ管理を希望するための登録を行った各機器は、認証管理部との間で無線ネットワークを形成し、所定の有効期限内だけ、認証管理部のセキュリティ管理下に置かれ、第三者の機器から盗聴されないようにすることができる。

【００１４】但し、この有効期限は、機器が認証管理部から付与される認証情報を使用することができる期間であり、機器は、認証情報の有効期限を更新するために、定期的に認証管理部に対して上記有効期限の更新を行う必要がある。このように認証情報の有効期限を設定するのは、機器が永続的に家庭内無線ネットワークに接続されないようにする必要があること、この機器が他者へ譲渡され、廃棄されたりしたときでも、ある時点でセキュリティ管理の有効期限が切れることによって、不用意に家庭内の無線ネットワークに接続される危険性を減らすことが可能なためである。

【００１５】具体的には、図２５に示すように、認証管理部Aは、機器１０ａ及び機器１０ｃのセキュリティ管理を行い、更に、認証管理部Bは、機器１０ｄ及び機器１０ｃのセキュリティ管理を行うものである。一方、認証管理部Ａは、屋外の機器１０ｂ及び隣家の機器１０ｆのセキュリティ管理を行わないようにし、更に、認証管理部Ｂは、屋外の機器１０ｆのセキュリティ管理を行わないようにする。このA家の機器１０ａ及び機器１０ｃが認証管理部Ａのセキュリティ管理下で通信を行うために

は、認証管理部Aから付与された認証情報を用いて通信を行うことにより実行することができる。また、認証管理部Ａ（又はＢ）は、認証管理部Ａ（又はＢ）が形成する無線ネットワーク（図２５中の点線の範囲内）の範囲内で、特定の機器１０ｎ及び機器１０ｃのセキュリティ管理を行うことができる。

【００１６】

【発明が解決しようとする課題】しかしながら、セキュリティ管理を行うことができる有効期限の終了時刻は、無線ネットワークを形成する範囲内に存在する各機器間で管理されているものであるが、無線ネットワークの範囲内に複数の機器が存在する場合は、各機器間で同一であるとは限らない。一般に有効期限の終了時刻が各機器間で同一でない理由としては、例えば、二つ機器のうち、片方の機器の方が先に新しい有効期限を更新しようとする場合があること、各機器の持つ時計の時刻が全く同一ではないことなどがあるためである。

【００１７】また、各機器が、自機の持つ時計の時刻で有効期限を判断する場合は、たとえある時点で時計の時刻が正確であったとしても、自機の内部に有するＣＰＵなどの構造上、時間が将来的に進んだり、遅れたりすることは避けられない。このため、機器間で秘密鍵の有効期限の開始時期が同一であったとしても、各機器の秘密鍵の有効期限は、将来的に同一時刻に終了しない場合がある。

【００１８】更に、家庭で使われる各機器は、必ずしも常時電源が入っているとは限らないため、各機器の電源が入っていないときには、次に電源が投入されるときまで認証情報の更新を受けることができない。この場合には、認証情報の更新を受けることができなかった機器は、電源が投入されてから認証情報の更新を受けるまでの遅延が発生し、その間は他の機器と異なる認証情報を持つ場合がある。

【００１９】従って、機器は、現時点で他の機器が有する秘密鍵と共通している場合であっても、上記より将来的に他の機器が有する秘密鍵と共通しなくなる場合があり、自機が有する秘密鍵を用いて他の機器との間で通信を行うことができなくなる可能性がある。

【００２０】各機器は、上記各機器が有する有効期限の終了時刻に差がある場合は、他の機器間で通信の開始をすることができない、或いは他の機器間で行っている通信が途中で中断されてしまうなどという問題が発生する。例えば、Bluetoothによる無線方式を用いた機器は、ポイント・ポイント間（機器間）の通信を行っているので、両方の機器間で認証情報を更新するタイミングが揃っていなければ通信が中断される。　また、IEEE 802.11無線LANのようなブロードキャスト型の無線方式を用いた機器は、通信に参加している機器の数を特定することは困難であるが、それら全ての機器が同じ認証情報を保有していない限り、通信が一部中断されてしまう可

能性がある。

【００２１】そこで、本発明は以上の点に鑑みてなされたもので、各機器が、各機器に有する秘密鍵の有効期限の終了時刻に差がある場合に、各機器間で行われる通信を開始することができなくなることを防止する機器認証管理システム及び機器管理方法を提供することを課題とする。

【００２２】

【課題を解決するための手段】本願に係る発明は上記課題を解決すべくなされたものであり、請求項１に係る発明は、所定の秘密情報を管理する認証管理手段から前記秘密情報を取得した機器が、取得した該秘密情報を用いて他の機器との間で通信をするための認証を行う機器認証管理システムであって、前記認証管理手段が、前記認証管理手段と前記機器との間で通信を行うための第一認証情報と、前記機器と他の機器との間で通信を行うための第二認証情報とを有する前記秘密情報を生成する生成手段と、前記生成手段で生成された前記第一認証情報を用いて、前記機器との間で通信をするための認証を行う第一認証手段と、前記第一認証手段の認証に基づいて前記第二認証情報を送信する第一通信手段とを有し、前記機器が、前記認証管理手段から予め取得してある前記第一認証情報を用いて、前記第一認証手段との間で通信をするための認証を行う第二認証手段と、前記第二認証部の認証に基づいて前記第一通信手段から前記第二認証情報を受信する第二通信手段とを有することを特徴とするものである。

【００２３】このような請求項１に係る発明によれば、機器は、認証管理手段から予め取得した第一認証情報を用いて認証管理手段との間で通信をするための認証を行うので、前記第一認証情報を有しなければ認証管理手段との間の通信を行うことができない。このため、認証管理手段は、第一認証情報を有していない機器との間では通信を行わないようにすることができ、第一認証情報を有しない機器からの不正なアクセスを排除することができる。

【００２４】また、請求項２に係る発明は、請求項１に記載の機器認証管理システムであって、前記第二認証手段が、前記第二通信手段で受信した第二認証情報を用いて、前記他の機器との間で通信をするための認証を行う機能を有し、前記第二通信手段が、前記第二認証手段の認証に基づいて、前記他の機器との間で通信を行う機能を有することを特徴とするものである。

【００２５】このような請求項２に係る発明によれば、機器は、第一認証情報を有していなければ、認証管理手段との間で通信を行うことができず第二認証手段を取得することができないので、第一認証情報を有していない機器は、認証管理手段から他の機器との間で通信を行うための第二認証情報を取得することができない。このため、認証管理手段は、第一認証情報を有していない機器には第二認証情報を送信しないので、第一認証情報を有しない機器から第二認証情報の不正要求があったとしても、前記不正要求をした機器に第二認証情報を送信しないようにすることができる。

【００２６】また、第二認証情報を有する機器は、第二認証情報を用いなければ他の機器との間で通信を行うことができないので、第二認証情報を有する他の機器との間では、その第二認証情報を媒介して無線ネットワークを形成することができる。このため、第二認証情報を媒介して無線ネットワークを形成した各機器は、第二認証情報を有しない機器からの通信を排除することができ、秘密文書などの情報データが第二認証情報を有しない機器に漏れることがない。

【００２７】また、請求項３に係る発明は、請求項１又は請求項２に記載の機器認証管理システムであって、前記第二認証情報が、該第二認証情報を識別するための識別子と、前記第二認証情報を使用することができる有効期限情報とを有することを特徴とするものである。

【００２８】このような請求項３に係る発明によれば、第二認証情報には、第二認証情報の有効期限が含められているので、第二認証情報を媒介して無線ネットワークを形成した各機器は、第二認証情報の有効期限が切れた機器を前記無線ネットワークから排除することができる。また、第二認証情報を有する機器が盗難された場合であっても、その機器を盗難された機器は、第二認証情報の有効期限が切れれば第二認証情報を有する機器との間で通信を行うことができないこととなる。

【００２９】このため、上記無線ネットワークを形成した各機器は、無線ネットワークに属する機器が盗難された場合であっても、その盗難された機器に有する第二認証情報の有効期限が切れれば、その盗難された機器を無線ネットワークから排除することができるので、無線ネットワーク内の情報データがいつまでも外部に漏れ出てしまうことを防ぐことができる。

【００３０】また、請求項４に係る発明は、請求項３に記載の機器認証管理システムであって、前記機器が、前記他の機器が有する複数の前記第二認証情報に含まれる前記識別子を取得し、その取得した前記識別子と、前記機器が有する複数の前記第二認証情報に含まれる前記識別子との間で共通する前記識別子を抽出して、その抽出した前記識別子に対応する前記第二認証情報のうち、該識別子に対応する前記有効期限情報に基づいて、該有効期限情報に対応する一つの前記第二認証情報を選定する第一選定手段と、前記第二認証手段が、前記第一選定手段で選定された第二認証情報に基づいて前記他の機器との間で通信をするための認証を行う機能を有することを特徴とするものである。

【００３１】このような請求項４に係る発明によれば、各機器は、選定手段が、他の機器が有する複数の第二認証情報に含まれる識別子を取得し、その取得した識別子と、機器が有している複数の第二認証情報に含まれる識別子との間で共通する前記識別子を抽出して、その抽出した前記識別子に対応する第二認証情報のうち、前記識別子に対応する有効期限情報に基づいて該有効期限情報に対応する一つの前記第二認証情報を選定することができるので、各機器に複数の第二認証情報を有する場合であっても、各機器に共通の第二認証情報を選ぶことができる。

【００３２】また、請求項５に係る発明は、請求項２又は請求項３に記載の機器認証管理システムであって、前記第二通信手段が前記認証管理手段から前記第二認証情報を取得した時間を、前記第二認証情報に付加する時間付加手段と、前記時間付加手段で前記時間が付加された前記第二認証情報を複数取得し、その前記時間が付加された複数ある前記第二認証情報の中から、付加された前記時間に基づいて、該時間に対応する一つの前記第二認証情報を選定する第二選定手段と、前記第二認証手段が、前記第二選定手段で選定された前記第二認証情報に基づいて、前記他の機器との間で認証を行う機能を有することを特徴とするものである。

【００３３】このような請求項５に係る発明によれば、選定手段が、時間付加手段で付加された時間（認証管理手段から第二認証情報を取得した時刻）に基づいて、前記時間に対応する第二認証情報を選ぶことができるので、第二認証情報の有効期限情報だけでなく、前記時間を用いることによっても第二認証情報を選ぶことができる。

【００３４】また、請求項６に係る発明は、請求項２に記載の機器認証管理システムであって、前記第二認証情報を所定の周期毎に生成する前記生成手段と、前記生成手段で所定の周期毎に生成された前記第二認証情報を複数取得し、その複数取得した前記第二認証情報の個数が所定の個数を超えたときは、取得した複数ある前記第二認証情報のうちのいずれかを削除する第三選定手段とを有することを特徴とするものである。

【００３５】このような請求項６に係る発明によれば、第三選定手段が、生成手段で所定の周期毎に生成された第二認証情報を複数取得し、その複数取得した第二認証情報の個数が所定の個数を超えたときは、取得した複数ある前記第二認証情報のうちのいずれかを削除することができるので、機器は、第二認証情報の有効期限を管理する必要がなくなり、更に、有効期限を管理するための時間管理部（図示せず）を設ける必要がない。

【００３６】また、請求項７に係る発明は、所定の認証情報を管理する認証管理手段から前記認証情報を取得した機器が、取得した該認証情報を用いて他の機器との間で通信をするための認証を行う機器認証管理方法であって、前記認証管理手段が、前記認証管理手段と前記機器との間で通信を行うための第一認証情報と、前記機器と他の機器との間で通信を行うための第二認証情報とを有する前記秘密情報を生成するステップと、生成された前記第一認証情報を用いて、前記機器との間で通信をするための認証を行うステップと、前記機器との間で通信をするための認証に基づいて前記第二認証情報を送信するステップとを有し、前記機器が、前記認証管理手段から予め取得してある前記第一認証情報を用いて、前記認証管理手段との間で通信をするための認証を行うステップと、前記認証管理手段との間で通信をするための認証に基づいて、前記認証管理手段から前記第二認証情報を受信するステップとを有することを特徴とするものである。

【００３７】このような請求項７に係る発明によれば、機器が、認証管理手段から予め取得した第一認証情報を用いて認証管理手段との間で通信をするための認証を行うので、前記第一認証情報を有しなければ認証管理手段との間の通信を行うことができない。このため、認証管理手段は、第一認証情報を有していない機器との間では通信を行わないようにすることができ、第一認証情報を有しない機器からの不正なアクセスを排除することができる。

【００３８】また、請求項８に係る発明は、請求項７に記載の機器認証管理方法であって、前記機器が、前記認証管理手段から受信した第二認証情報を用いて、前記他の機器との間で通信をするための認証を行うステップと、前記他の機器との間で通信をするための認証に基づいて、前記他の機器との間で通信を行うステップとを有することを特徴とするものである。

【００３９】このような請求項８に係る発明によれば、第二認証情報を有する機器が、第二認証情報を用いなければ他の機器との間で通信を行うことができないので、第二認証情報を有する他の機器との間では、その第二認証情報を媒介して無線ネットワークを形成することができる。このため、第二認証情報を媒介して無線ネットワークを形成した各機器は、第二認証情報を有しない機器からの通信を排除することができ、秘密文書などの情報データが第二認証情報を有しない機器に漏れないようにすることができる。

【００４０】また、請求項９に係る発明は、請求項７又は請求項８に記載の機器認証管理方法であって、前記第二認証情報は、前記第二認証情報を識別するための識別子と、前記第二認証情報を使用することができる有効期限情報とを有することを特徴とするものである。

【００４１】このような請求項９に係る発明によれば、第二認証情報には、第二認証情報の有効期限が含められているので、第二認証情報を媒介して無線ネットワークを形成した各機器は、第二認証情報の有効期限が切れた機器を前記無線ネットワークから排除することができる。また、第二認証情報を有する機器が盗難された場合であっても、その機器を盗難された機器は、第二認証情報の有効期限が切れれば第二認証情報を有する機器との

間で通信を行うことができないこととなる。

【0042】また、請求項10に係る発明は、請求項9に記載の機器認証管理方法であって、前記機器が、前記他の機器が有する複数の前記第二認証情報に含まれる前記識別子を取得し、その取得した前記識別子と、前記機器が有する複数の前記第二認証情報に含まれる前記識別子との間で共通する前記識別子を抽出して、その抽出した前記識別子に対応する前記第二認証情報のうち、該識別子に対応する前記有効期限情報に基づいて、該有効期限情報に対応する一つの前記第二認証情報を選定するステップと、選定された前記第二認証情報に基づいて、前記他の機器との間で通信をするための認証を行うステップとを有することを特徴とするものである。

【0043】このような請求項10に係る発明によれば、機器が、他の機器が有する複数の第二認証情報に含まれる識別子を取得し、その取得した識別子と、機器が有している複数の第二認証情報に含まれる識別子との間で共通する前記識別子を抽出して、その抽出した前記識別子に対応する第二認証情報のうち、前記識別子に対応する有効期限情報に基づいて該有効期限情報に対応する一つの前記第二認証情報を選定することができるので、各機器に複数の第二認証情報を有する場合であっても、各機器に共通の第二認証情報を選ぶことができる。

【0044】また、請求項11に係る発明は、請求項8又は請求項9に記載の機器認証管理方法であって、前記機器が、前記認証管理手段から前記第二認証情報を取得した時間を、前記第二認証情報に付加するステップと、前記時間が付加された前記第二認証情報を複数取得し、その前記時間が付加された複数ある前記第二認証情報の中から、付加された前記時間に基づいて、該時間に対応する一つの前記第二認証情報を選定するステップと、選定された前記第二認証情報に基づいて、前記他の機器との間で認証を行うステップとを有することを特徴とするものである。

【0045】このような請求項11に係る発明によれば、機器は、時間付加手段で付加された時間（認証管理手段から第二認証情報を取得した時刻）に基づいて、前記時間に対応する第二認証情報を選ぶことができるので、第二認証情報の有効期限情報だけでなく、前記時間を用いることによっても第二認証情報を選ぶことができる。

【0046】

【発明の実施の形態】〔第一実施形態〕

（機器認証管理システムの構成）本発明の実施形態について図面を参照しながら説明する。図2は、本実施形態に係る機器認証システムの内部構造を示したものである。同図に示すように、機器認証システムは、所定の秘密情報を管理する認証管理部20から秘密情報を取得した機器10aが、取得した秘密情報を用いて他の機器10bとの間で通信をするための認証を行うものである。

【0047】ここで、認証管理部20は、認証管理部20と機器10との間で通信を行うための第一認証情報と、機器10と他の機器10との間で通信を行うための第二認証情報からなる秘密情報を生成する秘密情報生成部22と、秘密情報生成部22で生成された第一認証情報を用いて、機器10との間で通信をするための認証を行う認証部26と、認証部26の認証に基づいて第二認証情報を送信する通信部25とを備えている。

【0048】また、機器10は、認証管理部20から予め取得してある第一認証情報を用いて、認証部26との間で通信をするための認証を行う認証部16と、認証部16の認証に基づいて通信部25から第二認証情報を受信する通信部14とを備えている。

【0049】即ち、機器認証システムは、図1に示すように、認証管理部20からマスタ鍵Ma～Mcを取得した各機器10a～10cが、取得したマスタ鍵Ma～Mcを用いて、各機器10a～10cに共通する共通鍵Kを認証管理部20から取得し、その共通鍵Kを取得した各機器10a～10cは、取得した共通鍵Kを用いて、情報データの送受信を行いたい各機器10a～10cとの間で認証をする。この共通鍵Kを用いて認証が成功した各機器10a～10cは、認証が成功した各機器の相互間で情報データを送受信することができる。

【0050】上記マスタ鍵Mは、認証管理部20と機器10との間で通信を行うための第一認証情報（暗号キー）である。また、共通鍵Kとは、第二認証情報（認証情報）の一部であり、機器10と他の機器10との間で通信を行うための暗号キーを意味するものである。

【0051】また、認証情報は、機器10と他の機器10との間で通信を行うための第二認証情報であり、例えば、各機器10との間で共通の暗号認証を行うための共通鍵K（暗号キー）と、認証情報を識別するための識別子と、認証情報の有効期限を示す有効期限情報とを有している。更に、秘密情報は、第一認証情報と第二認証情報とを含めたものを意味する。

【0052】図2に示すように、本実施形態に係る機器認証システムは、機器10と、認証管理部20とを有している。

【0053】前記機器10は、認証管理部20から所定の秘密情報を取得し、その取得した秘密情報を用いて他の機器10との間で通信をするための認証を行うものであり、本実施形態では、操作部11と、取得情報蓄積部12と、取得情報管理部13と、通信部14と認証情報決定部15と、認証部16とを有している。

【0054】操作部11は、情報データなどの入力を行うものであり、例えば、キーボードなどが挙げられる。尚、操作部11の形状としては、ボタン形状のものや、ジョイスティック型ものなどが挙げられる。具体的に操作部11は、認証管理部20に機器10の情報を登録するための検知信号を検知した場合は、その検知した検知信号を取得情報管理部13へと出力する。

【0055】また、操作部11は、ユーザの操作により認証管理部20との間で認証を行うための認証命令信号を検知した場合は、その検知した認証命令信号を取得情報管理部13へと出力する。更に、操作部11は、ユーザの操作により各機器10との間で認証を行うための機器認証命令信号が入力された場合は、入力された機器認証命令信号を取得情報管理部13へと取得する。

【0056】取得情報蓄積部12は、第一認証情報（マスタ鍵M）、或いは第二認証情報（認証情報）を複数蓄積する情報蓄積手段であり、例えば、ハードディスク、ICチップなどが挙げられる。具体的に取得情報蓄積部12は、取得情報管理部13が通信部14から取得したマスタ鍵M、或いは認証情報を蓄積する。尚、取得情報蓄積部12には、他の機器10に送信する文字、顔画像などの情報データも蓄積することができる。

【0057】取得情報管理部13は、機器10の内部動作を制御するものであり、例えば、CPUなどが挙げられる。具体的に取得情報管理部13は、操作部11から検知信号が入力された場合は、入力された検知信号に基づいて、検知信号に対応する登録情報を作成する。そして、登録情報を作成した取得情報管理部13は、その作成した登録情報を要求信号として通信部14へと出力する。

【0058】ここで、登録情報には、例えば、機器10の名称、機器10を所有するユーザの写真、機器10を製造販売するメーカ名、機器10のシリアル番号、ユーザが機器10を購入した年月日、PIN（Personal Identification Number）などが挙げられる。この機器10の登録情報を認証管理部20に登録することにより、機器10は、認証管理部20からマスタ鍵Mを取得することができる（詳述は後述する）。

【0059】通信部14から要求信号を受信した認証管理部20は、受信した要求信号に基づいて、その要求信号を送信した機器10を認証管理部20の無線ネットワークに属するようにするための登録をし、その登録を行った機器10にマスタ鍵Mを配布する。取得情報管理部13は、認証管理部20から送信されたマスタ鍵Mを通信部14で受信した場合は、受信したマスタ鍵Kを取得情報蓄積部12に蓄積する。

【0060】また、操作部11から認証命令信号が入力された取得情報管理部13は、入力された認証命令信号を通信部14に送信すると共に、入力された該認証命令信号に対応するマスタ鍵Mを取得情報蓄積部12から取得し、その取得したマスタ鍵Mを認証部16へと出力する。取得情報管理部13から認証命令信号が入力された通信部14は、入力された認証命令信号を通信部25に送信する。

【0061】取得情報管理部13から認証命令信号に対応するマスタ鍵Mが入力された認証部16は、入力されたマスタ鍵Mを用いて、認証管理部20にある通信部25から送信されたマスタ鍵Mで暗号化された共通鍵Kを復号化し、その復号化した共通鍵Kを取得情報管理部13へと出力する。

【0062】認証部16から復号化された共通鍵Kが入力された取得情報管理部13は、入力された共通鍵Kを取得情報蓄積部12に蓄積する。更に、操作部11から機器認証命令信号が入力された取得情報管理部13は、入力された機器認証命令信号を認証情報決定部15へと出力する。

【0063】認証情報決定部15は、他の機器10との間で通信をするための第二認証情報を選定するものであり、本実施形態では、有効期限判断部15aと、順序部15bと、選定部15cとを有している。

【0064】有効期限判断部15aは、第二認証情報（認証情報）に含まれる有効期限情報を確認するものである。具体的に有効期限判断部15aは、取得情報管理部13から機器認証命令信号が入力された場合は、取得情報蓄積部12に蓄積されている共通鍵Kを取得し、その取得した共通鍵Kに基づいて、その共通鍵Kに含まれている有効期限情報から共通鍵Kの有効期限（終了時期）を判断し、その有効期限を判断したことを示す判断信号を取得情報管理部13と、順序部15bとへ出力する。

【0065】順序部15bは、第二認証情報に含まれる有効期限情報に基づいて、その有効期限情報に対応する複数の第二認証情報を所定の順番に並び換えるものである。具体的に順序部15bは、有効期限判断部15aから判断信号が入力された場合は、入力された判断信号に基づいて、取得情報蓄積部12に蓄積されている複数ある認証情報を、例えば有効期限が近い順番に並び換え、その並び換えた結果を示す並び換え結果信号を選定部15cへと出力する。

【0066】選定部15cは、取得情報蓄積部12に複数蓄積されている有効期限情報を含む第二認証情報の中から、該第二認証情報に含まれる有効期限情報に基づいて、該有効期限情報に対応する一つの第二認証情報を選定する選定手段である。具体的に選定部15cは、順序部15bから並び換え結果信号が入力された場合は、入力された並び換え結果信号に基づいて、並び換えられた認証情報のうち、どの認証情報を使用するかを判断し、その判断した結果を使用判断信号として取得情報管理部13へと出力する。

【0067】例えば、並び換え結果信号信号が入力された選定部15cは、入力された並び換え結果信号に基づいて、有効期限順に並び換えられた認証情報のうち、有効期限の終了時期が長い認証情報を、各機器10との間の認証に使用するなどと判断する。

【0068】また、選定部15は、他の機器10bに有する複数の第二認証情報（共通鍵K）に含まれる識別子を取

格し、その取得した鍵対データと、機器１０ａに有する鍵対の第二認証用個体識別情報に含まれる鍵対データとの照合を共通するデータ鍵Ｋｎ－１を用いて、その他の暗号化方式に対応する第二認証情報のうち、録鍵対データに対応する前記有効期限情報に基づいて録対効期限情報に対応する一つの前記第二認証情報を選定する第一選定手段である。

【００６９】具体的には、光ディスク装置１１（機器１０ａにある装作部１１）が、ユーザの操作による機器１０ｂからの機器認証命令信号を検知したら録対は、操作部１１は、その検知した機器認証命令信号を取得情報管理部１３に出力する。

【００７０】操作部１１から機器認証命令信号が入力された取得情報管理部１３は、入力された機器認証情報を識別子に基づいて認証情報を選ぜべき信号であると判断した場合は、その入力された機器認証命信号を識別子（ｎ－３，ｎ－２，ｎ－１）として出力する。尚、取得情報管理部１３は、入力された機器認証命信号が認証情報に含まれる有効期限情報に基づいて認証情報を選ぜべき信号であると判断した場合は、その入力された機器認証命信号を上記有効期限判断部１５ａに出力する。

【００７１】取得情報管理部１３から機器認証命令信号が入力された選定部１５ｃは、入力された機器認証命令信号に基づいて、例えば、機器認証命令信号に対応する認証情報を選ぜする手段である。

【００７２】選定部１５ｃから鍵対データ（ｎ－３，ｎ－２，ｎ－１，ｎ）が入力された通信部１４は、入力された鍵対データと同様に、例えば（ｎ－３，ｎ－２，ｎ－１，ｎ）を機器１０ｂの通信部14へと送信する。機器１０ｂの取得情報書換部１２に書換されている鍵対データ（ｎ－３，ｎ－２，ｎ－１，ｎ）を、認証手順と同様に、機器１０ｂは、上記手順と同様に、例えば（ｎ－３，ｎ－２，ｎ－１，ｎ）を送信する。

【００７３】機器１０ａの通信部14は、機器１０ｂから鍵対データ（ｎ－３，ｎ－２，ｎ－１）を受信した場合は、受信した鍵対データ（ｎ－３，ｎ－２，ｎ－１）を選定部15ｃへと出力する。そして、通信部１４から鍵対データ（ｎ－３，ｎ－２，ｎ－１）が入力された選定部15ｃは、自機が使用する認証情報の鍵対データ（ｎ－３，ｎ－２，ｎ－１，ｎ）を取得情報書換部１２から取得し、その取得した鍵対データ（ｎ－３，ｎ－２，ｎ－１）と、通信部１４から入力された鍵対データ（ｎ－３，ｎ－２，ｎ－１）とを比較する。

【００７４】両者の鍵対データを比較すると、鍵対データ（ｎ－３，ｎ－２，ｎ－１）は、一致しているので、選定部１５ｃは、例えば、その一致している鍵対データ（ｎ－３，ｎ－２，ｎ－１）のうち、有効期限データが一番長い鍵対データｎ－１を選定する。また、この鍵対データｎ－１の選定は、機器１０ｂにある光ディスク装置１４ｃでも、上記同様の手順により行われる。

【００７５】鍵対データｎ－１を選定した選定部１５ｃは、選定情報の鍵対データと、通信部１４から入力された鍵対データ（ｎ－３，ｎ－２，ｎ－１）とを取得情報書換部１２から取得し、その取得した鍵対データ（ｎ－３，ｎ－２，ｎ－１）を、機器１０ｂの通信部14へと送信する。

【００７６】尚、選定部15ｃは、秘密情報生成部22（生成手段）で所定の周期毎に生成された第二認証情報を照合し第二認証情報の個数が所定の個数を超えたときは、取得した照数ある第二認証情報のうちのいずれかを削除する第三選定手段であってもよい。これにより、機器は、第二認証情報の有効期限を管理するなど要することなく、常に、有効期限を管理するために、選定部15から機器１０ａと機器１０ｂとの間で共通する暗号方式（図示せず）を設ける必要がない。

【００７７】認証部１６は、認証管理部２０から取得して入力される第一認証情報（マスタ鍵Ｍ）を用いて、認証部２６との間で通信をするための認証を行う第二認証手段である。具体的に認証部１６で行う認証は、図３に示すように、無線ネットワークプロトコルのＯＳＩを用いて認証することができる。同図によれば、機器１０ａと機器１０ｂとの間で共通の共通鍵Ｋは、先ず、認証管理部２０にあるＯＳＩのアプリケーション層で、共通鍵Ｋを定した鍵対データｎ－１に対応する共通鍵Ｋｎ－１を、取得情報書換部１２から取得し、その取得した共通鍵Ｋｎ－１を、秘密情報生成部22で生成する（詳述は後述する）。

【００７８】マスタ鍵Ｍで暗号化された共通鍵Ｋを取得した機器１０ａ（通信部１４で取得）は、機器１０ａにある認証部１６にあるＯＳＩのアプリケーション層で、マスタ鍵Ｍで暗号化された共通鍵Ｋを、取得情報管理部１３へと出力する。共通鍵Ｋは、取得情報管理部１３から復号化した認証部１６は、復号化した共通鍵Ｋを取得情報書換部２１に書換されている鍵対データｎ－１（ｎ－３，ｎ－２，ｎ－１）を、機器１０ｂに送信する。機器１０ｂは、上記手順と同様に、例えば（ｎ－３，ｎ－２，ｎ－１）を機器１０ｂの通信部14へと送信する。

【００７９】また、認証部１６は、通信部14で受信した第二認証情報（共通鍵Ｋ）を用いて、他の機器10ｂとの間で通信を行う第二認証手段でもある。具体的に認証部１６は、機器１０ａと機器１０ｂとの間で通信をするための認証を行う場合は、選定部15から機器１０ａと機器１０ｂとの間で共通の共通鍵Ｋを取得し、その取得した共通鍵Ｋを取得した認証部１６は、ＯＳＩのデータリンク層で暗号化された情報データを取得した機器10ｂの認証部26は、共通鍵Ｋで暗号化された情報データを復号する。機器１０ａから共通鍵Ｋで暗号化されたデータを取得した機器１０ｂの認証部26は、共通鍵Ｋを用いて復号する。

ータを、機器１０ｂが予め有している共通鍵Ｋを用いて復号化する。

【００８１】これにより、認証管理部２０に登録した全ての機器１０ａ（１０ｂ）～と配布されるのマスタ鍵Ｍを取得情報書換部１２に書換する。

【００８２】また、通信部１４は、取得情報管理部１３から要求信号が入力された場合は、認証管理部２０に対して、機器１０ａと機器１０ｂとの間で通信を行うための第一認証用個体識別情報（共通鍵Ｋ）とを生成する生成手段である。

【００８３】通信部１４から入力された取得情報書換部１２は、入力されたマスタ鍵Ｍを取得情報管理部１３へと出力する。

【００８４】通信部１４からマスタ鍵Ｍで暗号化された認証情報を、取得情報管理部１３から入力されたマスタ鍵Ｍを用いて復号化し、その復号化したマスタ鍵Ｍを取得情報書換部２１に書換する。

【００８５】また、通信部１４は、取得情報管理部１３から要求信号が入力された場合は、認証管理部２０に送信する。

【００８６】通信部１４からマスタ鍵Ｍが入力された取得情報管理部１３は、入力されたマスタ鍵Ｍを取得情報書換部２１に書換する。その後、操作部１１からの機器認証命令信号が入力された取得情報管理部１３は、入力された機器認証命令信号に基づいて、マスタ鍵Ｍを取得情報書換部２１から取得し、その取得したマスタ鍵Ｍ＿Ｘ１またはマスタ鍵Ｍ＿Ｘ２を通信部１４へと出力する。

【００８７】また、通信部１４は、認証部１６の認証に基づいて、他の機器１０ｂの通信を行う第二通信手段でもある。具体的に通信部１４は、認証部16から共通鍵Ｋで暗号化された情報データが入力された場合は、入力された共通鍵Ｋで暗号化された情報データを他の機器１０ｂに送信する。

【００８８】前記認証管理部２０は、所定の秘密情報を管理するもので、図１に示すように、本実施形態では、操作部２１と、秘密情報生成部２２と、秘密情報書

０ａ及び１０ｂに共通する共通鍵Ｋを取得するために、マスタ鍵Ｍｃを要求する要求信号を認証管理部２０に送信した場合は、認証管理部２０は、その受信した要求信号に対応するマスタ鍵Ｍｃを機器１０ｃに送信する。

【００９６】認証管理部２０からマスタ鍵Ｍｃを受信した機器１０ｃは、図６に示すように、マスタ鍵Ｍｃで暗号化された共通鍵Ｋを認証管理部２０から受信し、その受信したマスタ鍵Ｍｃで暗号化された共通鍵Ｋを、前に取得したマスタ鍵Ｍｃを用いて復号化する。これにより、共通鍵Ｋを復号化した機器１０ｃは、同図に示すように、機器１０ｃに有する共通鍵Ｋを用いて、共通鍵Ｋを有する機器１０ａ及び機器１０ｂの間で形成される無線ネットワークに属することができる。

【００９７】秘密情報生成部22は、図７に示すように、機器１０に用いられている通信方式に応じてマスタ鍵Ｍの種類を設定することができる。例えば、秘密情報生成部２１は、同図中のＢＴ機器１０ａ及び機器１０ｂがBluetoothによる通信方式を用いている場合は、Bluetoothによる通信方式に対応したマスタ鍵M_{B1}及びマスタ鍵M_{B2}を生成することができる。

【００９８】認証管理部２０からマスタ鍵M_{B1}又はマスタ鍵M_{B2}を取得したＢＴ機器１０ａ及び１０ｂは、認証管理部２０から送信されたマスタ鍵M_{B1}又はマスタ鍵M_{B2}で暗号化された共通鍵Ｋ１（Bluetoothによる通信方式を用いた機器１０間で認証を行うキー）を、前に取得したマスタ鍵M_{B1}及びマスタ鍵M_{B2}を用いて復号化し、その復号化した共通鍵Ｋ１を用いてＢＴ機器１０ａ及びＢＴ機器１０ｂの間で認証をする。

【００９９】一方、秘密情報生成部22は、同図中の８０２．１１機器１０ｃ～１０ｅが８０２．１１による通信方式を用いている場合は、８０２．１１による通信方式に対応したマスタ鍵M_{81}～M_{83}を生成することができる。認証管理部２０からそれぞれマスタ鍵M_{81}～M_{83}を取得した８０２．１１機器１０ｃ～１０ｅは、認証管理部２０からマスタ鍵M_{81}～M_{83}で暗号化された共通鍵Ｋ２を受信し、前に取得したマスタ鍵M_{81}～M_{83}を用いて復号化し、その復号化した共通鍵Ｋ２を用いて８０２．１１機器１０ｃ～１０ｅとの間で認証をする。

【０１００】これにより、秘密情報生成部２１は、機器１０で採用されている通信方式に応じてマスタ鍵Ｍを生成することができるので、各機器１０は、自機で採用されている通信方式に応じたマスタ鍵Ｍを取得することができ、更に、自機が採用している通信方式と同一である他の機器１０との間で無線ネットワークを形成することができる。

【０１０１】また、認証管理部２０は、上記よりＩＥＥＥ８０２．１１、Bluetooth、HiperLAN2などの通信方式が異なる機器１０毎にマスタ鍵Ｍの種類を換えることによって、通信方式が異なる複数の機器１０を管理することができる。更に、ＣＰＵスペックが小さく、リアルタイムクロックを持たない機器１０は、各機器１０間で共通の認証情報などを生成することなどが困難であるが、認証管理部２０から送信されるマスタ鍵Ｍを用いることによって各機器１０間との間の無線ネットワークを簡単に形成することができる。

【０１０２】秘密情報管理部24は、認証管理部２０の内部動作を制御するものである。具体的に通信部２５から要求信号が入力された秘密情報管理部２４は、入力された要求信号を秘密情報生成部22へと出力する。尚、認証管理部２０への登録とは、登録情報に対応するマスタ鍵Ｍが秘密情報管理部２３に蓄積されたことを意味する。

【０１０３】また、秘密情報管理部24は、秘密情報生成部２２から要求信号に対応する生成されたマスタ鍵Ｍ、或いは認証情報が入力された場合は、入力されたマスタ鍵Ｍ、認証情報、登録情報を秘密情報蓄積部23に蓄積する。更に、通信部２５から認証命令信号が入力された秘密情報管理部２４は、入力された認証情報命令信号に基づいて、その認証命令信号に対応するマスタ鍵Ｍと共通鍵Ｋとを秘密情報蓄積部２３から取得し、その取得したマスタ鍵Ｍと共通鍵Ｋとを認証部２６へと出力する。

【０１０４】秘密情報蓄積部23は、秘密情報生成部22で生成された秘密情報（マスタ鍵Ｍ、認証情報）を蓄積するものであり、例えば、ハードディスクなどが挙げられる。具体的に秘密情報蓄積部23は、秘密情報管理部24からマスタ鍵Ｍ、認証情報、登録情報が入力された場合は、入力されたマスタ鍵Ｍ、認証情報、登録情報を蓄積する。

【０１０５】通信部25は、認証部26の認証に基づいて第二認証情報（認証情報）を送信する第一通信手段であり、例えば、Bluetoothによる通信方式を用いた通信機器、IrDAによる通信方式を用いた通信機器などが挙げられる。具体的に通信部１４から要求信号（或いは認証命令信号）を受信した通信部25は、受信した要求信号（或いは認証命令信号）を秘密情報管理部24へと出力する。また、秘密情報管理部２４から要求信号に対応するマスタ鍵Ｍが入力された通信部２５は、入力されたマスタ鍵Ｍを、要求信号を送信した通信部１４に送信する。

【０１０６】認証部26は、秘密情報生成部22で生成された第一認証情報を用いて、機器１０との間で通信をするための認証を行う第一認証手段である。具体的に認証部26は、秘密情報管理部24から認証命令信号に対応するマスタ鍵Ｍと認証情報とが入力された場合は、入力された認証情報をマスタ鍵Ｍで暗号化し、そのマスタ鍵Ｍで暗号化した認証情報を通信部26に出力し、認証部２６からマスタ鍵Ｍで暗号化された認証情報が入力された通信部２５は、入力されたマスタ鍵Ｍで暗号化された認証情報を機器１０に送信する。尚、認証部26で行われている内部処理は、上述した認証部16と同様の内部処理が行われている。

【０１０７】（機器認証管理システムを用いた機器認証管理方法）上記構成を有する機器認証管理システムによる機器認証管理方法は、以下の手順により実施することができる。図８は、本実施形態に係る機器認証管理方法の全体のフロー（状態遷移）を示したものである。尚、同図中における丸く囲まれている部分は、機器１０の状態を意味しており、また四角で囲まれている部分は、処理を意味している。

【０１０８】同図に示すように、認証管理方法は、所定の認証情報を管理する認証管理部２０から認証情報を取得した機器１０が、取得した認証情報を用いて他の機器１０との間で通信をするための認証を行うものである。

【０１０９】先ず、機器１０が認証管理部２０に登録されていない場合は、機器１０は、自機の登録情報を認証管理部２０に登録することを行う（Ｓ１、Ｓ２）。機器１０を認証管理部２０に登録すると、その登録された機器は、認証管理部２０からマスタ鍵Ｍを取得することができる（Ｓ３）。そして、認証管理部２０からマスタ鍵Ｍで暗号化した共通鍵Ｋを取得した機器１０は、その取得したマスタ鍵Ｍで暗号化された共通鍵Ｋを、ステップＳ３で取得したマスタ鍵Ｍを用いて共通鍵Ｋへと復号化して共通鍵Ｋを取得する（Ｓ５～Ｓ９）。

【０１１０】その後、機器１０は、復号化した共通鍵Ｋを用いて、他の機器１０との間で認証を行い、認証が成功した他の機器１０との間で情報データを送受信する（Ｓ１０～Ｓ１２）。尚、認証管理部２０で登録された機器１０を削除するのは、認証管理部２０で蓄積されている登録情報に対応するマスタ鍵Ｍを削除することにより行う（Ｓ１３～Ｓ１５）。上記に示す、機器認証方法を構成する各手順の詳述は、以下の手順により説明することができる。

【０１１１】（１）機器１０が、認証管理部２０からマスタ鍵Ｍと共通鍵Ｋとを取得する方法

図９は、機器１０が認証管理部２０からマスタ鍵Ｍと共通鍵Ｋとを取得する手順を示したものである。同図に示すように、先ず、機器１０が認証管理部２０に対して登録情報を送信するステップを行う（Ｓ１０１）。具体的には、取得情報管理部１３が、操作部１１から検知信号が入力された場合は、入力された検知信号に基づいて、その検知信号に対応する登録情報を作成する。

【０１１２】そして、機器１０がマスタ鍵Ｍを取得するためには、操作部１１及び操作部２１の両者においてユーザの操作（この操作には認証情報の入力、例えばＰＩＮの入力が含まれる）が必要である。取得情報管理部１３は操作部１１から検知信号が入力された場合、要求信号（これには登録情報は含まれない）を通信部を経由して認証管理部２０に送信する。

【０１１３】一方、認証管理部２０は操作部２１に検出信号があった場合、機器１０から上記要求信号が送信されるまで待機する。ただし上記要求信号を既に受信している場合は除く。操作部２１に検出信号がある前に上記要求信号を受信した場合は、認証管理部２０は機器１０から上記要求信号が送信されるまで待機する。

【０１１４】（上記段落に記載のいずれかの方法で）機器１０から要求信号を受信し、かつ操作部２１に検出信号があった後で、認証管理部２０は認証手順開始要求を機器１０に送信し、認証管理部２０と機器１０の間の認証手順を開始する。

【０１１５】この認証手順の具体的な内容はここでは定義しないが、例えば機器１０が操作部１１にユーザの入力したＰＩＮとその他登録情報を認証管理部２０に送信し、認証管理部２０はこのＰＩＮを操作部２１にユーザが入力したＰＩＮと比較する、方法がある。又は、機器１０と認証管理部２０の間でDiffie-Hellman鍵交換等の方法により（一時的な）鍵の生成を最初に行い、上記ＰＩＮとその他登録情報の送信はこの鍵により暗号化して行うこともできる。更に、（後述する）マスタ鍵Ｍの送信も、ここで生成した鍵を使って行うことができる。この鍵は登録手順（図９の手順）が完了すると廃棄される。

【０１１６】認証手順が成功した場合のみ（ＰＩＮが一致しない等の理由で失敗した場合は登録を続行しない）、以下のマスタ鍵Ｍの生成等が行われる。尚、ここでは原則として操作部１１と操作部２１の両方でユーザの操作を要求することにしたが、別の例としては、どちらか一方の操作を省略する方法であってもよい。例えば、機器１０のＰＩＮは製造時に割り当てられた固定の値にし、これを操作部２１に入力することにより行うことができる。この場合要求信号は機器１０ではなく、認証管理部２０が機器１０に向けて送信する。

【０１１７】次いで、認証管理部２０が、機器１０との間で認証を行うためのマスタ鍵Ｍを生成し、その生成したマスタ鍵Ｍを該当する機器１０に送信するステップを行う（Ｓ１０２）。具体的には、通信部１４から要求信号を受信した通信部２５は、受信した要求信号を秘密情報管理部２４へと出力する。そして、通信部２５から要求信号が入力された秘密情報管理部２４は、入力された要求信号を秘密情報生成部２２へと出力する。

【０１１８】その後、秘密情報管理部２４から要求信号が入力された秘密情報生成部22は、入力された要求信号に基づいて、その要求信号に対応するマスタ鍵Ｍを生成する。マスタ鍵Ｍを生成した秘密情報生成部２１は、生成したマスタ鍵Ｍを秘密情報管理部24へと出力すると共に、その生成したマスタ鍵Ｍのみを通信部２５へと出力する。秘密情報生成部22からマスタ鍵Ｍが入力された秘密情報管理部24は、入力されたマスタ鍵Ｍと登録情報とを秘密情報蓄積部23へと蓄積する。尚、認証管理部２０が機器１０を登録するとは、登録情報に対応するマスタ鍵Ｍを秘密情報蓄積部２３に蓄積することを意味する。

【０１１９】そして、秘密情報生成部２２からマスタ鍵Ｍが入力された通信部２５は、入力されたマスタ鍵Ｍ

23

を、要求信号を送信した通信部１４へと送信する。その後、通信部２５からマスタ鍵Mを受信した通信部１４は、受信したマスタ鍵Mを取得情報管理部１３へと出力し、通信部１４からマスタ鍵Mが入力された取得情報管理部１３は、入力されたマスタ鍵Mを取得情報蓄積部１２に蓄積する。

【０１２０】尚、認証管理部２０は定期的に共通鍵Kを生成するので、その直後に認証管理部２０から転送開始の要求を行う。このときに通信可能でない機器１０がある可能性もあるので、このタイミング以外でもときどき（例えば、定期的に）転送開始の要求を行ってもよい。

【０１２１】これにより認証管理部２０は、どの機器１０に共通鍵Kの転送を行ったかどうか、というリストの管理を省くことが可能となる。更に、共通鍵Kに有効期限情報が設定されているとき、機器１０が自身の持つ共通鍵Kの有効期限が切れるおそれがあると判断した場合にも、機器１０の側から転送開始の要求をしてもよい。

【０１２２】次いで、機器１０が、認証管理部２０から共通鍵Kを取得するステップを行う（Ｓ１０３）。具体的には、取得情報管理部１３は、認証命令信号を通信部１４に送信すると共に、マスタ鍵Mを取得情報蓄積部１２から取得し、その取得したマスタ鍵Mを認証部１６へと出力する。取得情報管理部１３から認証命令信号が入力された通信部１４は、入力された認証命令信号を通信部２５に送信する。

【０１２３】その後、通信部１４から認証命令信号を受信した通信部25は、受信した認証命令信号を秘密情報管理部24へと出力する。そして、通信部２５から認証命令信号が入力された秘密情報管理部２４は、入力された認証情報命令信号に基づいて、その認証命令信号に対応するマスタ鍵Mと認証情報とを秘密情報蓄積部２３から取得し、その取得したマスタ鍵Mと認証情報とを認証部２６へと出力する。

【０１２４】そして、秘密情報管理部24から認証命令信号に対応するマスタ鍵Mと認証情報とが入力された認証部２６は、入力された認証情報をマスタ鍵Mで暗号化し、そのマスタ鍵Mで暗号化した認証情報を通信部２５に出力し、認証部２６からマスタ鍵Mで暗号化された認証情報が入力された通信部２５は、入力されたマスタ鍵Mで暗号化された認証情報を機器１０に送信し、通信部１４は、通信部２５から送信されたマスタ鍵Mで暗号化された認証情報を受信する。

【０１２５】次いで、取得情報管理部１３から認証命令信号に対応するマスタ鍵Mが入力された認証部１６は、入力されたマスタ鍵Mを用いて、通信部１４で受信したマスタ鍵Mで暗号化された共通鍵Kを復号化し、その復号化した共通鍵Kを取得情報管理部１３へと出力する。そして、認証部１６から復号化された共通鍵Kが入力された取得情報管理部１３は、入力された共通鍵Kを取得情報蓄積部１２に蓄積する。

24

【０１２６】そして、機器１０が、共通鍵Kで形成された無線ネットワークに参加する場合は、上記復号化した共通鍵Kを各機器１０間の認証に用いることにより、共通鍵Kで形成された無線ネットワークに参加することができる（Ｓ１０４）。

【０１２７】尚、認証管理部２０に登録してある機器１０の登録を削除する方法は、図１０に示すように、先ず、機器１０が、認証管理部２０に対して、登録を削除するための削除情報を送信するステップを行う（Ｓ２０１）。ここで、機器１０の登録を削除するとは、秘密情報蓄積部23に蓄積されている登録情報に対応するマスタ鍵Mを削除することを意味する。

【０１２８】具体的には、操作部１１が、ユーザの操作により認証管理部２０に登録してある機器１０の登録を削除するための信号を検知した場合は、認証管理部２０に登録してある機器１０の登録を削除するための検知信号を、取得情報管理部１３に出力する。そして、操作部１１から検知信号が入力された取得情報管理部１３は、入力された検知信号に基づいて、認証管理部２０に登録してある機器１０の登録を削除するための登録削除信号を生成し、その生成した登録削除信号を通信部１４へと出力する。その後、取得情報管理部１３から登録削除信号が入力された通信部１４は、入力された登録削除信号を該当する通信部２５に送信する。

【０１２９】その後、秘密情報管理部２４は、マスタ鍵Mを削除するステップを行う（Ｓ２０２）。具体的には、通信部１４から登録削除信号を受信した通信部２５は、受信した登録削除信号を秘密情報管理部24へと出力する。更に、通信部２５から登録削除信号が入力された秘密情報管理部24は、入力された登録削除信号に基づいて、登録削除信号に対応するマスタ鍵Mを秘密情報蓄積部２３から削除する。尚、マスタ鍵Mは、認証管理部２０にある操作部２１を介して削除することもできる。

【０１３０】次いで、認証管理部２０は、秘密情報管理部２２が機器１０に対応するマスタ鍵Mを削除しているので、登録削除信号を送信した機器１０に共通鍵Kを送信しないようにする（Ｓ２０３）。その後、機器１０は、認証管理部２０からマスタ鍵Mで暗号化された新たな共通鍵K'を取得することができないので、予め取得してある共通鍵Kの有効期限が切れたと同時に、共通鍵K'で形成された無線ネットワークに属することができなくなる。

【０１３１】即ち、機器１０は、認証管理部２０から共通鍵Kを取得したとしても、その取得した共通鍵Kに有効期限が設定されていれば、その共通鍵Kの有効期限が切れたと同時に、共通鍵Kで形成された無線ネットワークに属することができなくなる。

【０１３２】（２）機器１０が、認証管理部２０から取得した複数ある認証情報（共通鍵K1～K３）のうち、認証情報に含まれる有効期限情報（共通鍵Ｋ１～Ｋ３に

25

対応する有効期限情報Ｔ１～Ｔ３）に基づいて、他の機器との間で認証する際に使用する一つの共通鍵を選定する方法

図１１は、機器１０が、取得情報蓄積部１２に蓄積されている複数の認証情報のうち、認証情報に含まれる有効期限情報に基づいて、他の機器１０との間で認証を行う際に使用する一つの共通鍵を選定する手順を概念的に示したものである。同図に示すように、機器１０ｃは、取得情報蓄積部１２にある取得情報テーブルに複数の認証情報を蓄積している。

【０１３３】機器１０ｃが、機器１０ａ又は機器１０ｂとの間で認証の際に使用する共通鍵Ｋ１～Ｋ３のいづれかを選定する方法は、例えば、取得情報蓄積部１２に蓄積されている認証情報のうち、有効期限Ｔ３が長い共通鍵Ｋ３を選定する方法がある。尚、ＴｎとＫｎにある添え文字ｎは、１、２、３・・・・の数字を意味するものである。

【０１３４】取得情報蓄積部１２に蓄積されている認証情報は、同図に示すように、認証情報の識別子ｎ３～ｎ１に対応する有効期限Ｔ３～Ｔ１（この順番は有効期限が長い順番）と共通鍵Ｋ３～KIとを有している。このため、機器１０ｃにある選定部１５ｃは、取得情報蓄積部１２に蓄積されている共通鍵Ｋ１～Ｋ３のうち、有効期限が一番長い共通鍵を選定すると設定している場合は、有効期限が一番長いＫ３を選定することになる。この共通鍵の選定方法は、具体的には以下の通りである。

【０１３５】先ず、操作部１１が、ユーザに操作部１１を操作させることにより、各機器１０との間で認証を行うための機器認証命令信号を検知した場合は、その操作部１１は、その検知した機器認証命令信号を取得情報管理部１３へと出力する。そして、操作部１１から機器認証命令信号が入力された取得情報管理部１３は、入力された機器認証命令信号を有効期限判断部１５ｎへと出力する。

【０１３６】その後、取得情報管理部１３から機器認証命令信号が入力された有効期限判断部１５ａは、取得情報蓄積部１２に蓄積されている認証情報（共通鍵Ｋ１～Ｋ３）を取得し、その取得した認証情報に基づいて、その共通鍵Ｋ１～Ｋ３に含まれている有効期限情報Ｔ１～Ｔ３から共通鍵Ｋ１～Ｋ３の有効期限を判断し、その有効期限を判断したことを示す判断信号を取得情報管理部１３と、順序部１５ｂとへ出力する。

【０１３７】そして、有効期限判断部１５ａから判断信号が入力された順序部１５ｂは、入力された判断信号に基づいて、取得情報蓄積部１２に蓄積されている複数ある認証情報を、例えば有効期限が近い順番に並び換え、その並び換えた結果を示す並び換え結果信号を選定部15ｃへと出力する。

【０１３８】次いで、順序部１５ｂから並び換え結果信号が入力された選定部15ｃは、入力された並び換え結果

26

信号に基づいて、並び換えられた認証情報のうち、有効期限が一番長い認証情報（共通鍵Ｋ３）を使用すると判断し、その使用すると判断した認証情報を認証部１６へと出力する。

【０１３９】そして、選定部１５ｃから共通鍵Ｋ３が入力された認証部１６は、入力された共通鍵Ｋ３に基づいて、機器１０ｎ及機器１０ｂとの間の認証を行う（図１１参照）。尚、上記手順は、複数の認証情報に含まれる有効期限情報に基づいて、機器１０ｎ（１０ｂ）で用いる認証情報を選定（他の機器１０ｎ及び機器10ｂは、単数の認証情報）したが、後述する手順（３）は、認証情報に含まれる識別子に基づいて、他の機器間で用いる認証情報を選定することもできる。また、後述する手順（３）は、両機器に有する認証情報の数が複数でも両者に共通する認証情報を選定することができる。

【０１４０】（３）機器１０ｎが、認証情報に含まれる識別子に基づいて他の機器１０ｂとの間で用いる認証情報を選定し、その選定した認証情報を用いて他の機器１０ｂとの間で通信を行う方法

図１２は、機器１０ｎが他の機器１０ｂとの間で共通鍵Ｋを用いて情報データを送受信する方法を示したものである。同図に示すように、先ず、機器１０ｎが、他の機器１０ｂに対して、使用することが可能な共通鍵Ｋの識別子ｎを送信するステップを行う（Ｓ３０１）。具体的には、先ず、操作部１１（機器１０にある操作部１１）が、ユーザの操作により機器１０ｂとの間で認証を行うための機器認証命令信号を検知した場合は、操作部１１は、その検知した機器認証命令信号を取得情報管理部１３へと出力する。

【０１４１】そして、操作部１１から機器認証命令信号が入力された取得情報管理部１３は、入力された機器認証命令信号を選定部１５ｃに出力し、取得情報管理部１３から機器認証命令信号が入力された選定部１５ｃは、入力された機器認証命令信号に基づいて、機器認証命令信号に対応する識別子ｎ（認証情報の一部）を取得情報蓄積部１２から取得し、その取得した識別子ｎを通信部１４へと出力する。その後、取得情報管理部１３から識別子ｎが入力された通信部１４は、入力された識別子ｎを機器１０ｂの通信部へと送信する。

【０１４２】一方、機器１０ｂは、上記手順（Ｓ３０２）と同様に、機器１０ｂの取得情報蓄積部１２ｂに蓄積されている識別子ｎｂを、識別子ｎを送信した機器１０ｎに送信するステップを行う（Ｓ３０２）。その後、機器１０ｎは、自機の取得情報蓄積部１２に蓄積されている識別子ｎと、機器１０ｂから受信した識別子ｎｂ（機器１０ｂが所有している共通鍵Ｋｂの識別子）とを比較し、両者が一致している場合は、識別子ｎに対応する共通鍵Ｋを用いて機器１０ｂに送信する情報データを暗号化するステップを行う（Ｓ３０３）。

【０１４３】具体的には、機器１０ｎにある通信部１４

ａが、機器１０ｂから識別子ｎｂを取得し、その取得した識別子ｎｂを選定部15ｃへと出力する。そして、通信部１４ａから識別子ｎｂが入力された使用部１０ｃは、自機が使用する共通鍵Ｋ（使用する共通鍵Ｋを選定する方法は、上記（２）を参照のこと）の識別子ｎを取得情報蓄積部１２から取得し、その取得した識別子ｎと、通信部から入力された識別子ｎｂとを比較し、その両者を比較した結果、両者が一致していれば、識別子ｎに対応する共通鍵Ｋを認証部１６へと出力する。

【０１４４】尚、選定部１５ｃが、機器１０ａと機器１０ｂの識別子を比較し、その両者を比較した結果、複数の識別子が一致していれば、その一致している複数の識別子（ｎ〜ｎ-2）に対応する認証情報のうち、その識別子（ｎ〜ｎ-2）に対応する有効期限情報に基づいて、例えば有効期限が長い識別子ｎに対応する認証情報Knを選定する（図１３参照）。

【０１４５】その後、選定部15ｃから識別子ｎに対応する共通鍵Ｋが入力された認証部１６は、入力された共通鍵Ｋを用いて、機器１０ｂに送信する情報データを暗号化し、その共通鍵Ｋで暗号化された情報データを機器１０ｂへと送信する（Ｓ３０３）。機器１０ａから共通鍵Ｋで暗号化された情報データを受信した機器１０ｂの認証部は、受信した共通鍵Ｋで暗号化された情報データを、自機が有する識別子ｎｂに対応する共通鍵Ｋｂ（機器１０ａの共通鍵Ｋと同じ）を用いて復号化（Ｓ３０４）し、機器１０ａから送信された情報データを取得する。

【０１４６】これにより、機器１０ａは、機器１０ａにある情報データを、共通鍵Ｋを用いて暗号化して機器１０ｂに送信することができるので、認証管理部２０を介在させなくても情報データを送信することができる。

【０１４７】尚、図１３に示すように、機器１０ａ〜１０ｃが複数の共通鍵Ｋｎ〜Ｋｎ-2を有している場合は、上記と同様の手順により、例えば、機器１０ａは、有効期限が一番長いＫｎを用いて他の機器１０ｂ及び機器１０ｃに情報データを送信することができる。機器１０ａが他の機器１０ｂ及び１０ｃに情報データを送信する方法（複数の機器に情報データを送信する場合）は、上記の手順と同様に行うことができる。また、上記説明は、ある時点において両機器10a（１０ｂ）に有する認証情報が同一である場合についての手順を示したものである。

【０１４８】（４）機器１０ａ及び１０ｂが、ある時点において両機器１０ａ（１０ｂ）に有している認証情報が同一でない場合の通信方法

（３）の方法では、ある時点において各機器１０に有している共通鍵Ｋが同一である場合の通信方法について説明したが、（４）では、ある時点において各機器１０に有している共通鍵Ｋが同一でない場合の通信方法について説明する。図１４は、ある時点において、機器１０ａ及び機器１０ｂに有する共通鍵Ｋが異なる場合の通信方法の概要を示したものである。

【０１４９】同図に示すように、ある時点において機器１０ａ及び機器１０ｂにある共通鍵Ｋの種類が異なると、機器１０ａと機器１０ｂとは、両者の間で情報データを送受信することができなくなる。このため、機器１０ａ及び機器１０ｂは、以下の手順による方法で機器１０ａと機器１０ｂとの間で用いる共通鍵Ｋを選定し、その選定された共通鍵Ｋを用いて機器１０ａと機器１０ｂとの間で情報データの送受信を行う。

【０１５０】同図に示すように、認証管理部２０では、共通鍵をKn-3、Kn-2、Kn-1、Ｋｎの順序で生成し、機器１０ａ及び機器１０ｂでは、認証管理部２０で生成された各共通鍵Kn-3、Kn-2、Kn-1、Ｋｎを取得し、その取得した各共通鍵を取得情報蓄積部１２に蓄積する。但し、機器１０ａ及び機器１０ｂの取得情報蓄積部１２に蓄積されているある時点の共通鍵Ｋｎ〜Ｋｎ-3の種類は、異なるものとする（同図参照）。また、同図に示す取得情報テーブルとは、取得情報蓄積部１２に蓄積されている認証情報（識別子ｎ、有効期限Ｔ、共通鍵Ｋなど）を時系列の順番で示したものである（時系列は上の段から始まるものとする）（「取得情報テーブル」は、以下同じ意味を有するものとする）。

【０１５１】そして、機器１０ａ及び機器１０ｂは、取得情報蓄積部１２に蓄積されている共通鍵のうち、機器１０ａ又は機器１０ｂとの間で用いる共通鍵を選定し、その選定された共通鍵を用いて機器１０ａ又は機器１０ｂに有する情報データを送受信する。

【０１５２】図１５〜図１７は、機器１０ａ及び機器１０ｂが両機器１０ａ（１０ｂ）間で使用する認証情報の選定順序を時系列で示したものである。以下の手順は、時系列により取得情報テーブルに蓄積されている共通鍵を用いて通信を行うことを示したものである。

【０１５３】図１５及び図１６に示すように、機器１０ａが、取得情報蓄積部１２に蓄積されている共通鍵Ｋｎ-1を用いて機器１０ｂとの間で通信を行う（Ｓ４０１ａ）には、先ず、機器１０ａが、他の機器１０ｂに対して、使用することが可能な共通鍵（Kn-1〜Kn-3）の識別子（ｎ-1〜n-3）を送信するステップを行う（Ｓ５０１ａ、Ｓ５０２ａ）。

【０１５４】具体的には、先ず、操作部１１（機器１０ａにある操作部１１）が、ユーザの操作により機器１０ｂとの間で認証を行うための機器認証命令信号を検知した場合は、操作部１１は、その検知した機器認証命令信号を取得情報管理部１３へと出力する。

【０１５５】そして、操作部１１から機器認証命令信号が入力された取得情報管理部１３は、入力された機器認証命令信号を選定部１５ｃに出力し、取得情報管理部１３から機器認証命令信号が入力された選定部１５ｃは、入力された機器認証命令信号に基づいて、機器認証命令信号に対応する認証情報の識別子（n-3、n-2、ｎ-1、ｎ）を取得情報蓄積部１２から取得し、その取得した識別子（n-3、n-2、ｎ-1、ｎ）を通信部１４へと出力する。

【０１５６】その後、取得情報管理部１３から識別子（n-3、n-2、ｎ-1、ｎ）が入力された通信部１４は、入力された識別子（n-3、n-2、ｎ-1、ｎ）を機器１０ｂの通信部14へと送信する。一方、機器１０ｂは、上記手順と同様に、機器１０ｂの取得情報蓄積部１２に蓄積されている識別子（n-3、n-2、ｎ-1）を、識別子（n-3、n-2、ｎ-1、ｎ）を送信した機器１０ａに送信する（Ｓ５０１ｂ、Ｓ５０２ｂ）。

【０１５７】次いで、機器１０ａは、自機の取得情報蓄積部１２に蓄積されている識別子（n-3、n-2、ｎ-1、ｎ）と、機器１０ｂから受信した識別子（n-3、n-2、ｎ-1）とを比較し、両者が一致している場合は、機器１０ｂに送信する情報データを暗号化する（Ｓ５０３ａ〜Ｓ５０５ａ）。

【０１５８】具体的には、機器１０ａにある通信部１４が、通信部２５から識別子（n-3、n-2、ｎ-1）を取得し、その取得した識別子（n-3、n-2、ｎ-1）を選定部15ｃへと出力する。そして、通信部１４ａから識別子（n-3、n-2、ｎ-1）が入力された選定部１５ｃは、自機が使用する共通鍵Ｋに対応する識別子（n-3、n-2、ｎ-1、ｎ）を取得情報蓄積部１２から取得し、その取得した識別子（n-3、n-2、ｎ-1、ｎ）と、通信部１４から入力された識別子（n-3、n-2、ｎ-1）とを比較する。

【０１５９】両者の識別子を比較すると、両者の識別子（n-3、n-2、ｎ-1）は、一致しているので、選定部１５ｃは、例えば、その一致している識別子（n-3、n-2、ｎ-1）のうち、有効期限Ｔが一番長い識別子ｎ-1を選定する。また、この識別子ｎ-1の選定は、機器１０ｂにある選定部１５ｃでも、上記同様の手順により行われる（Ｓ５０３ｂ〜Ｓ５０５ｂ）。このため、機器１０ｂにある選定部１５ｃは、有効期限Ｔが一番長い識別子ｎ-1を選定することになる。

【０１６０】その後、識別子ｎ-1を選定した選定部１５ｃは、選定した識別子ｎ-1に対応する共通鍵Ｋｎ-1を、取得情報蓄積部１２から取得し、その取得した共通鍵Ｋｎ-1を認証部１６へと出力する。そして、選定部15ｃから識別子ｎ-1に対応する共通鍵Kn-1が入力された認証部１６は、入力された共通鍵Kn-1を用いて、機器１０ｂに送信する情報データを暗号化し、その共通鍵Kn-1で暗号化された情報データを機器１０ｂへと送信する。

【０１６１】更に、機器１０ａから共通鍵Kn-1で暗号化された情報データを受信した機器１０ｂの認証部２６は、受信した共通鍵Kn-1で暗号化された情報データを、自機が有する識別子n-1に対応する共通鍵Kn-1を用いて復号化し、機器１０ａから送信された情報データを取得する（Ｓ５０６ａ、Ｓ５０７ａ、Ｓ５０６ｂ、Ｓ５０７ｂ）。

【０１６２】次いで、機器１０ａが、取得情報テーブル１２ａにある認証情報のうち、有効期限の切れた共通鍵Kn-3を検出するステップを行う（Ｓ４０２ａ）。具体的には、有効期限判断部１５ａが、認証情報に含まれる有効期限情報に基づいて、取得情報テーブル１２ａにある認証情報のうち、有効期限が切れた共通鍵Kn-3を検知し、その検知したことを示す共通鍵検知信号を取得情報管理部１３へと出力する。尚、Ｓ４０２ａのステップは、必ずしも機器１０ａと機器１０ｂ間の通信の状態には依存しない。随時共通鍵Ｋの有効期限が切れると判断されたときに行われる。

【０１６３】そして、有効期限判断部１５ａから共通鍵検知信号が入力された取得情報管理部１３は、入力された共通鍵検知信号に基づいて、新しい共通鍵を要求するための共通鍵要求信号を通信部１４へと出力する。その後、有効期限判断部１５ａから共通鍵要求信号が入力された通信部１４は、入力された共通鍵要求信号を認証管理部２０へと送信する。

【０１６４】尚、認証情報（共通鍵Ｋ）は、定期的に生成されるものである。具体的には、秘密情報生成部22がCPU（図示せず）で管理されている時間情報（時刻）に基づいて認証情報を逐次生成し、その生成した認証情報を秘密情報蓄積部23に蓄積する（Ｓ４０１ｃ）。

【０１６５】次いで、認証管理部２０が、機器１０ａからの要求により、Ｓ４０１ｃで生成済みの新しい共通鍵Ｋｎを機器１０ａに送信するステップを行う（Ｓ４０２ｃ、Ｓ７０１ａ〜Ｓ７０４ａ）。具体的には、通信部１４から共通鍵要求信号を受信した認証管理部２０は、受信した共通鍵要求信号を秘密情報管理部24へと出力する。そして、通信部２５から共通鍵要求信号が入力された秘密情報管理部２４は、入力された共通鍵要求信号に基づいて、共通鍵要求信号に対応する共通鍵Ｋｎを秘密情報蓄積部23から取得し、共通鍵Ｋｎを通信部２５へと出力する。そして、秘密情報管理部２２から共通鍵Ｋｎが入力された通信部２５は、入力された共通鍵Knを、共通鍵要求信号を送信した機器１０ａに送信する。

【０１６６】更に、認証管理部２０から共通鍵Ｋｎを受信した機器１０ａの通信部１４は、受信した共通鍵Ｋｎを取得情報管理部１３へと出力し、通信部１４から共通鍵Ｋｎが入力された取得情報管理部１３は、入力された共通鍵Ｋｎを取得情報蓄積部１３に蓄積する。ここで、秘密情報管理部２２は、入力された共通鍵Ｋｎを、有効期限が長い順に蓄積する（同図の取得情報テーブル１２ａ’を参照のこと）。尚、有効期限の切れた共通鍵Kn-3は、取得情報テーブル１２ａ’から削除してもよい。

【０１６７】次いで、取得情報テーブル１２ａ’を有する機器１０ａと取得情報テーブル１２ｂを有する機器１０ｂとの間の通信（Ｓ４０２ａ、Ｓ７０１ｂ〜Ｓ７０３ｂ）は、以下の手順により行われる（このＳ４０２ａの

31 32

手順は、Ｓ４０１ａの手順と基本的には同様である）。

【０１６８】具体的には、先ず、機器１０ａにある通信部１４ａが、機器１０ｂから識別子（n-3、n-2、n-1）を取得し、その取得した識別子（n-3、n-2、n-1）を選定部15ｃへと出力する。そして、通信部１４ａから識別子（n-3、n-2、n-1）が入力された選定部１５ｃは、自機が使用する共通鍵Ｋに対応する識別子（n-2、n-1、n）を取得情報蓄積部１２から取得し、その取得した識別子（n-2、n-1、n）と、通信部１４から入力された識別子（n-3、n-2、n-1）とを比較する。

【０１６９】両者の識別子のうち、識別子（n-2、n-1）は、一致しているので、選定部１５ｃは、例えば、その一致している識別子（n-2、n-1）のうち、有効期限Ｔが一番長い識別子ｎ-1を選定する。また、この識別子ｎ-1の選定は、機器１０ｂにある選定部１５ｃでも、上記同様の手順により行われる。

【０１７０】その後、識別子ｎ-1を選定した選定部１５ｃは、選定した識別子ｎ-1に対応する共通鍵Ｋｎ-1を、取得情報蓄積部１２から取得し、その取得した共通鍵Ｋｎ-1を認証部１６へと出力する。そして、選定部15ｃから識別子ｎ-1に対応する共通鍵Kn-1が入力された認証部１６は、入力された共通鍵Kn-1を用いて、機器１０ｂに送信する情報データを暗号化し、その共通鍵Kn-1で暗号化された情報データを機器１０ｂへと送信する。

【０１７１】そして、機器１０ａから共通鍵Kn-1で暗号化された情報データを受信した機器１０ｂの認証部は、受信した共通鍵Kn-1で暗号化された情報データを、自機が有する識別子n-1に対応する共通鍵Kn-1を用いて復号化し、機器１０ａから送信された情報データを取得する。

【０１７２】次いで、機器１０ｂが、取得情報テーブル１２ｂにある認証情報のうち、有効期限の切れた共通鍵Kn-3を検出するステップを行う（Ｓ４０１ｂ）。具体的には、有効期限判断部１５ａが、認証情報に含まれる有効期限情報に基づいて、取得情報テーブル１２ｂにある認証情報のうち、有効期限が切れた共通鍵Kn-3を検知し、その検知したことを示す共通鍵検知信号を取得情報管理部１３へと出力する。

【０１７３】そして、有効期限判断部１５ａから共通鍵検知信号が入力された取得情報管理部１３は、入力された共通鍵検知信号に基づいて、新しい共通鍵を要求するための共通鍵要求信号を通信部１４へと出力する。その後、有効期限判断部１５ａから共通鍵要求信号が入力された通信部１４は、入力された共通鍵要求信号を認証管理部２０へと送信する。

【０１７４】次いで、認証管理部２０が、機器１０ｂからの要求により、共通鍵Ｋｎを機器１０ｂに送信するステップを行う（Ｓ４０３ｃ）。具体的には、通信部１４から共通要求信号を受信した認証管理部２０は、受信した共通要求信号を秘密情報管理部２４へと出力する。そして、通信部２５から共通要求信号が入力された秘密情報管理部２４は、入力された共通要求信号に基づいて、共通要求信号に対応する共通鍵Ｋｎを秘密情報蓄積部23から取得し、共通鍵Ｋｎを通信部２５へと出力する。そして、秘密情報管理部２２から共通鍵Ｋｎが入力された通信部２５は、入力された共通鍵Knを、共通鍵要求信号を送信した機器１０ｂに送信する。

【０１７５】更に、認証管理部２０から共通鍵Ｋｎを受信した機器１０ｂの通信部１４は、受信した共通鍵Ｋｎを取得情報管理部１３へと出力し、通信部１４から共通鍵Ｋｎが入力された取得情報管理部１３は、入力された共通鍵Ｋｎを取得情報蓄積部１３に蓄積する。ここで、秘密情報管理部２２は、入力された共通鍵Ｋｎを、有効期限が長い順に蓄積する（同図の取得情報テーブル１２ｂ'を参照のこと）。尚、有効期限の切れた共通鍵Kn-3は、取得情報テーブル１２ｂ'から削除してもよい。

【０１７６】次いで、機器１０ｎが、共通鍵Knを用いて機器１０ｂとの間の通信を行うステップを行う（Ｓ４０３ａ）。このステップ（Ｓ４０３ａ）は、上述したステップ（Ｓ４０１ａ）と同様の手順を行うので、ステップ（Ｓ４０３ａ）の説明は、省略する。

【０１７７】これにより、機器１０ａ及び機器１０ｂが、認証管理部２０から新しい共通鍵を取得し、ある時点において取得情報テーブル１２ａ（１２ｂ）にある共通鍵が異なった場合であっても、機器１０ａ及び機器１０ｂは、取得情報テーブル１２ａ（１２ｂ）に蓄積された両機器に共通する共通鍵を使用することができるので、共通鍵が通信途中で更新されたとしても通信状態が途中で途切れることなく、機器１０ａ又は機器１０ｂから情報データを取得することができる。

【０１７８】一方、機器１０ａが、認証管理部２０から共通鍵を更新し続け、機器１０ａと機器１０ｂとの間で共通する共通鍵がなくなってしまった場合は、機器１０ａは、機器１０ｂとの間で共通の共通鍵を有しないので、機器１０ｂとの間の通信を行うことができなくなる。このため、機器１０ａが、機器１０ａと機器１０ｂとの間で共通の共通鍵を有しなくなり、両機器１０ａ（１０ｂ）は、機器１０ｂとの間で形成されていた無線ネットワークが解除されるので、両機器１０ａ（１０ｂ）に共通の共通鍵を用いて情報データを送受信することができなくなる。

【０１７９】尚、機器１０が認証管理部２０から新しい共通鍵Ｋを取得する方法は、上述にも示したが、図１８に示す手順によっても行うことができる。同図では、機器１０が、認証管理部２０から共通鍵を取得し、その取得した共通鍵を取得情報テーブル１２ａに蓄積し、取得情報テーブル１２ａに蓄積されている共通鍵のうち、最も古い共通鍵を削除することを示したものである。この図１７に示す具体的な内部動作（認証部１６などの動作）は、上記に示した動作と同様である。

33 34

【０１８０】同図の左側に示した認証管理部２０は、一定の周期Ｔｒで時系列的に共通鍵Ｋｎ-２、Ｋｎ-１、Ｋｎを生成し、その生成された共通鍵Ｋｎ-２、Ｋｎ-１、Ｋｎを順次送信する。認証管理部２０から共通鍵Ｋｎ-２、Ｋｎ-１、Ｋｎを受信した機器１０は、受信した共通鍵Ｋｎ-２、Ｋｎ-１、Ｋｎをそれぞれ取得情報テーブル１２ａ～１２ａ'''に蓄積し、その取得情報テーブル１２ａ～１２ａ'''に蓄積されている共通鍵のうち、最も古い共通鍵を削除する（Ｓ６０１～Ｓ６０３）。

【０１８１】具体的には、選定部15ｃは、秘密情報生成部22（生成手段）で所定の周期毎に生成された第二認証情報を複数取得し、その複数取得した第二認証情報の個数が所定の個数を超えたときは、取得した複数ある第二認証情報のうちのいずれかを削除する。即ち、機器１０が同図中の時点１で受信した共通鍵Kn-2は、時点３を経過した後に取得情報テーブル12aから削除される。このため、取得情報テーブル１２ａに蓄積されている共通鍵の有効期限は２Ｔｒとなる。これにより、機器１０は、特定の周期Ｔｒが経過したときに所定の共通鍵を取得することができるので、内部に設置されている時計を用いて共通鍵の有効期限を計測する必要がない。

【０１８２】（機器認証管理システム及び機器認証管理方法による作用及び効果）このような本実施形態に係る機器認証管理システム及び機器認証管理方法によれば、機器１０は、認証管理部２０から予め取得した第一認証情報（マスタ鍵M）を用いて認証管理部２０との間で通信をするための認証を行うので、前記第一認証情報（マスタ鍵M）を有しなければ認証管理部２０との間の通信を行うことができない。このため、認証管理部２０は、第一認証情報を有していない機器との間では通信を行わないようにすることができ、第一認証情報を有しない機器１０からの不正なアクセスを排除することができる。

【０１８３】また、第二認証情報を有する機器１０は、第二認証情報を用いなければ他の機器との間で通信を行うことができないので、第二認証情報を有する他の機器１０との間では、その第二認証情報を媒介して無線ネットワークを形成することができる。このため、第二認証情報を媒介して無線ネットワークを形成した各機器１０は、第二認証情報を有しない機器１０からの通信を排除することができ、秘密文書などの情報データが第二認証情報を有しない機器１０に漏れることがない。

【０１８４】また、第二認証情報には、第二認証情報の有効期限が含められているので、第二認証情報を媒介して無線ネットワークを形成した各機器１０は、第二認証情報の有効期限が切れた機器１０を前記無線ネットワークから排除することができる。また、第二認証情報を有する機器１０が盗難された場合であっても、その機器１０を盗難した者は、第二認証情報の有効期限が切れれば第二認証情報を有する機器との間で通信を行うことができないこととなる。

【０１８５】このため、上記無線ネットワークを形成した各機器１０は、無線ネットワークに属する機器が盗難された場合であっても、その盗難された機器１０に有する第二認証情報の有効期限が切れれば、その盗難された機器を無線ネットワークから排除することができるので、無線ネットワーク内の情報データがいつまでも外部に漏れ出てしまうことを防ぐことができる。

【０１８６】更に、各機器１０は、選定部１５ｃが、他の機器１０が有する第二認証情報に含まれる識別子を取得し、その取得した識別子と、取得情報蓄積部１２に蓄積されている第二認証情報に含まれる識別子との間で共通する前記識別子を抽出して、その抽出した前記識別子に対応する有効期限情報に基づいて該有効期限情報に対応する前記第二認証情報を選定することができるので、各機器１０に複数の第二認証情報を有する場合であっても、各機器に共通の第二認証情報を選定することができる。

【０１８７】〔第二実施形態〕

（機器認証管理システムの構成）本発明の第二実施形態について図面を参照しながら説明する。図１９は、本実施形態に係る機器認証管理システムの内部構造を示したものである。同図は、第一実施形態に係る機器認証管理システムの内部構造（図２参照）とほぼ同じであるが、認証管理部２０に生成指示部２７と機器１０の通信部１４に時間付加部１７とを有している点で相違する。この相違する構造以外の構造は、第一実施形態と同じであるので、相違する構造以外の構造についての説明は、省略する。

【０１８８】第一実施形態では、選定部１５ｃが、認証情報（認証情報の識別子、共通鍵の有効期限、共通鍵）にある有効期限、或いは識別子に基づいて、どの認証情報を使用するのかを判断していたが、本実施形態では、選定部１５ｃは、認証管理部２０から認証情報を取得した時間と、取得した認証情報の有効期限とに基づいて、どの認証情報を使用するのかを判断するものである。具体的な説明は以下の通りである。

【０１８９】生成指示部２７は、秘密情報生成部22に対して、秘密情報の生成を所定の周期毎に指示するためのものである。具体的に生成指示部２７は、図２０に示すように、所定の周期Ｔｒが経過した場合は、秘密情報生成部22に共通鍵を生成させるための生成信号を出力する。生成指示部２７から生成信号が入力された秘密情報生成部22は、入力された生成信号に基づいて、新たな共通鍵Ｋを生成し、その生成した共通鍵Ｋを生成指示部２７へと出力する。

【０１９０】尚、同図に示す共通鍵K1～K5は、秘密情報生成部22が、生成指示部２７から特定の周期Ｔｒをもって順次入力された生成信号に基づいて、その生成信号に対応して順次生成された共通鍵を意味するものである。

35

【０１９１】秘密情報生成部22から共通鍵Ｋ1～Ｋ5が入力された生成指示部２７は、機器１０ａの要求とは関係なく生成指示部２７からの生成信号に応じて無条件に共通鍵Ｋ1、Ｋ２（ユーザから要求された共通鍵）を認証部26へと出力すると共に、入力された共通鍵Ｋ1～Ｋ5を秘密情報蓄積部23に蓄積する。生成指示部２７から共通鍵Ｋ1、Ｋ２が入力された認証部26は、入力された共通鍵Ｋ1、Ｋ２をマスタ鍵Ｍで暗号化し、その暗号化した共通鍵Ｋ１，Ｋ２を通信部25に出力し、暗号化した共通鍵Ｋ１，Ｋ２が入力された通信部25は、入力された共通鍵Ｋ１，Ｋ２を機器１０にある通信部１４へと送信する。

【０１９２】時間付加部１７は、通信部１４が認証管理部20から第二認証情報を取得した時間を、第二認証情報に付加する時間付加手段である。具体的に時間付加部１７は、通信部２５から共通鍵Ｋ1、Ｋ２を受信した場合は、その共通鍵Ｋ1、Ｋ２を受信した時間（時間情報）を付加し、その時間情報を付加した共通鍵Ｋ1、Ｋ２を取得情報管理部１３へと出力する。時間付加部１７から時間情報を付加した共通鍵Ｋ1、Ｋ２が入力された取得情報管理部１３は、入力された共通鍵Ｋ1、Ｋ２を取得情報蓄積部１２に蓄積する。

【０１９３】尚、図２０に示すように、秘密情報生成部22で生成された各共通鍵（Ｋ１、Ｋ２）を通信部１４で受信するタイミングは、秘密情報生成部22で各共通鍵（Ｋ１、Ｋ２）が生成された時点と比較すると多少遅延Ｔｄしている。この遅延Ｔｄが生ずる要因は、認証管理部２０と機器１０との間で行われる通信開始手順に時間がかかること、通信網が混雑していること、秘密情報生成部22で生成された時刻に機器１０の電源が入っておらず、機器１０が認証管理部２０に対して共通鍵を要求することができない状況にあることなどが挙げられる。

【０１９４】選定部１５ｃは、まず各共通鍵（Ｋ１，Ｋ２）を調べ、時間情報から1/2Tr経過しているものを除去する（Ｋ２だけが除去されＫ１が残る場合と、Ｋ１とＫ２のどちらも除去されず残る場合場合が考えられる）。次に、残された共通鍵の中から時間情報が最も遅い共通鍵を選定する（つまり、Ｋ１だけ残っている場合はこれが選ばれる。Ｋ１とＫ２の両方が残っている場合はＫ２が選ばれる。

【０１９５】尚、選定部15ｃは、時間付加部１７時間が付加された第二認証情報（認証情報）を複数取得し、その前記時間が付加された複数ある第二認証情報の中から、付加された前記時間に基づいて、該時間に対応する一つの第二認証情報を選定する第二選定手段である。具体的に選定部15ｃは、取得情報管理部１３からの指示により、取得情報蓄積部１２に蓄積されている時間情報が付加された共通鍵（Ｋ１、Ｋ２）を取得し、その取得した共通鍵（Ｋ１、Ｋ２）のうち、時間情報（認証管理部２０から取得した時刻）が早い共通鍵Ｋ１を選定することもできる。

36

【０１９６】（機器認証管理システムを用いた機器管理方法）上記構成を有する機器認証管理システムによる機器認証管理方法は、以下の手順により実施することができる。尚、機器１０が選定部15ｃで選定された共通鍵Ｋを用いて他の機器１０に情報データを送信する方法は、上記第一実施形態で述べた方法と同様に行われる。

【０１９７】（１）機器１０ａ及び機器１０ｂに有する選定部15ｃが、それぞれ認証管理部２０から同じ時間で取得した各共通鍵（Ｋ１、Ｋ２）を選定する場合

図２１は、機器１０ａ（１０ｂ）が、認証管理部２０から同じ時間で取得した共通鍵（Ｋ１～Ｋ５）を示したタイミングチャートを示したものである。以下の手順は、同図に示したタイミングチャートを用いて、機器１０ａ（１０ｂ）にある選定部15ｃが、認証管理部２０から同じ時間に取得した各共通鍵（Ｋ１、Ｋ２）を、時間付加部１７で付加された時間に基づいて選定する方法について以下説明したものである。

【０１９８】先ず、秘密情報生成部22が、所定の周期Ｔｒ毎に共通鍵を生成するステップを行う。具体的には、生成指示部２７が、図２１に示すように、所定の周期Ｔｒが経過した場合は、秘密情報生成部22に共通鍵（Ｋ1～K5）を生成させるための生成信号を出力する。そして、生成指示部２７から生成信号が入力された秘密情報生成部22は、入力された生成信号に基づいて、新たな共通鍵Ｋ１～Ｋ５を生成し、その生成した共通鍵Ｋ１～Ｋ５を生成指示部２７へと出力する。

【０１９９】次いで、認証管理部２０が、機器１０ａ（１０ｂ）に対して、新たに生成された共通鍵Ｋ１（本実施形態では、共通鍵は1つずつ生成しているが、認証管理部２０にある認証サーバ初期設定により（図20の左端時刻）複数同時生成もすることができる）を送信するステップを行う。具体的には、秘密情報生成部22から共通鍵Ｋ1～Ｋ5が入力された生成指示部２７が、入力された共通鍵Ｋ1（ユーザから要求された共通鍵）を認証部26へと出力すると共に、入力された共通鍵Ｋ1～Ｋ5を秘密情報蓄積部23に蓄積する。

【０２００】尚、認証管理部２０は、機器10ａ（１０ｂ）からの要求等により共通鍵を送信することもできる。この場合、共通鍵は秘密情報蓄積部２３から取得され、認証部２６に出力されます。

【０２０１】そして、生成指示部２７から共通鍵Ｋ1が入力された認証部26は、入力された共通鍵Ｋ1をマスタ鍵Ｍで暗号化し、その暗号化した共通鍵Ｋ１を通信部25に出力し、暗号化した共通鍵Ｋ１が入力された通信部25は、入力された共通鍵Ｋ１を機器１０にある通信部１４へと送信する。

【０２０２】次いで、機器１０ａ（１０ｂ）は、認証管理部２０から受信した共通鍵Ｋ１に基づいて、時間情報を付加するステップを行う。具体的には、時間付加部１

37

７が、通信部２５から共通鍵Ｋ1を受信した場合は、その共通鍵Ｋ1を受信した時間（時間情報）を付加し、その時間情報を付加した共通鍵Ｋ1を取得情報管理部１３へと出力する。そして、時間付加部１７から時間情報を付加した共通鍵Ｋ1、Ｋ２が入力された取得情報管理部１３は、入力された共通鍵Ｋ1、Ｋ２を取得情報蓄積部１２に蓄積する。

【０２０３】その後、操作部１１に機器認証命令信号が入力された場合は、選定部15ｃが、取得情報管理部１３からの指示により、取得情報蓄積部１２に蓄積されている時間情報が付加された共通鍵（Ｋ１、Ｋ２）を取得し、その取得した共通鍵（Ｋ１、Ｋ２）のうち、上記手順に従って１つを選択して認証部１６へと出力する。

【０２０４】尚、機器１０ａ及び機器１０ｂは、図２１に示すように、認証管理部２０から取得した共通鍵（Ｋ１、Ｋ２、Ｋ３）の取得時間（時間情報）が同一であり、同図中のタイミングａ－タイミングｂ間で使用する共通鍵Ｋ３が両機器１０ａ（１０ｂ）で共通している。このため、機器１０ａ及び機器１０ｂは、タイミングａ－タイミングｂ間では、機器１０ａ及び機器１０ｂ間で行われる情報データの通信を両者に共通する共通鍵Ｋ３を用いて行うことができる。

【０２０５】尚、図２２及び図２３は、機器１０ａ及び機器１０ｃに有する選定部15ｃが、それぞれ認証管理部２０から異なる時間で取得した各共通鍵（Ｋ１、Ｋ２）を用いて機器１０ａ（１０ｂ）間で通信を行うことを示したタイムチャートである。図２２中に示されているＴＤ1は、機器１０ａが認証管理部２０から取得した共通鍵の取得時間（時間情報）と、機器１０ｃが認証管理部２０から取得した共通鍵の取得時間（時間情報）との間の時間差を意味するものである。

【０２０６】同図に示すように、機器１０ｃが、認証管理部２０から共通鍵Ｋ３を取得してから、機器１０ａとの間で共通鍵Ｋ３を使用することができるまでの時間は1/2Ｔｒ－TD1である。このため、機器10aは、上記1/2Ｔｒ－TD1により、TD1が1/2Ｔｒよりも大きくなれば、自機が機器１０ｃに対して情報データを送信することができない時間が生じる。

【０２０７】従って、この場合、機器１０ａが機器１０ｃに対して情報データを送信する際には、機器１０ｃにある選定部15ｃは、タイミングａ－タイミングｂ間では、機器１０ａで使用される共通鍵Ｋ３に対応させるために、共通鍵Ｋ３を使用する時間を、図中のｐ点より1/2Ｔｒ早めるように設定（以下、単に「マージン」と略す）する。これにより、タイミングａ－タイミングｂ間における共通鍵Ｋ３が、機器１０ａと機器１０ｃとの間で同じくなり、機器１０ａと機器１０ｃは、共通鍵Ｋ３を用いて情報データを送受信することができる。尚、機器１０ｃは、上記Ｔｄ1が1/2Ｔｒよりも小さければ、機器１０ａとの間で情報データを送信することができる。

38

【０２０８】また、図２３は、図２２とは逆に、機器１０ｃが、機器１０ａに対して情報データを送信する場合についてのタイミングチャートを示したものである。上記内容と同様に、機器10ｃは、タイミングｃ－タイミングｄ間では、図２３中の1/2Ｔｒ－TD2により、TD2が1/2Ｔｒよりも大きくなれば、自機が機器１０ａに対して情報データを送信することができない時間が生じる。

【０２０９】従って、この場合、機器１０ｃが機器１０ａに対して情報データを送信する際には、機器１０ａにある選定部15ｃは、タイミングｃ－タイミングｄ間では、機器１０ｃで使用される共通鍵Ｋ３に対応させるために、共通鍵Ｋ３の使用を終了する時間を、図中のｑ点より1/2Ｔｒ遅らせるように設定（以下、単に「マージン」と略す）する。これにより、タイミングｃ－タイミングｄ間における共通鍵Ｋ３が、機器１０ａと機器１０ｃとの間で同じくなり、機器１０ａと機器１０ｃは、共通鍵Ｋ３を用いて情報データを送受信することができる。尚、機器１０ｃは、上記Ｔｄ1が1/2Ｔｒよりも小さければ、機器１０ａとの間で情報データを送信することができる。

【０２１０】また、機器１０ａ（１０ｂ）は、機器１０ａ（１０ｂ）がｎ個の共通鍵を有する場合は、認証管理部２０からｎ個の共通鍵を取得してから1/2Ｔｒ（ｎ－1）［上手順の一般式］以上の時間が経過した秘密情報のうち、最も新しい共通鍵を使用する。このため、機器１０ａ（１０ｂ）は、機器１０ａ及び１０ｂとの間で共通鍵を取得する時刻に差があるときは、共通鍵を使用することができる時間に1/2Ｔｒ（ｎ－1）時間（上記「マージン」の一般式）のマージンを与えれば、機器１０ａ（１０ｂ）に有する共通鍵が等しくなり機器１０ａ及び機器１０ｂ間で情報データを送受信することができる。

【０２１１】図２４は、無線方式Ａと無線方式Ｂとが異なる場合であっても、無線方式Ａの機器１０ａと無線方式Ｂの機器１０ｂとに有している共通鍵の有効期限がほぼ同等であることを示したものである。

【０２１２】同図に示すように、無線方式Ａの機器１０ａに有している共通鍵（K_{A1}～K_{An}）の有効期限は、T_Aで更新されていくが、無線方式Ｂの機器１０ｂに有している共通鍵（K_{B1}～K_{B0}）の有効期限は、T_Aの2/3倍の周期（T_B）で更新される。このため、無線方式Ａの機器１０ａでは、タイミングｒ時点での共通鍵（K_{A1}，K_{A2}）の数を２つとし、無線方式Ｂの機器１０ｂでは、タイミングｒ時点での共通鍵の数を、上記機器１０ａの共通鍵数（K_{A1}，K_{A2}の２つ）の3/2倍である３つ（K_{B1}，K_{B2}，K_{B3}）にすれば、共通鍵（K_{A1}，K_{A2}）の有効期限と機器１０ｂの共通鍵（K_{B1}，K_{B2}）の有効期限とは、ほぼ同一になる（同図中の"Δｔ"は、機器１０ａと機器１０ｂとの共通鍵の有効期

39

限差が微差であることを意味している）。

【０２１３】従って、機器１０ｎ（１０ｂ）の共通鍵の有効期限は、機器１０ｎにある共通鍵の一部を削除し、或いは機器１０ｂにある共通鍵の一部を削除した場合であっても、上記のような更新周期（T_A．T_B）、共通鍵の数を設定すれば、ほぼ同一に扱うことができる。また、各機器１０ａ（１０ｂ）は、異なる無線方式が採用されている機器１０ａ（１０ｂ）の共通鍵や、その共通鍵の数が異なる場合であっても、上記に示すタイミングで共通鍵を更新することにより、各機器１０ａ（１０ｂ）にある共通鍵の有効期限をほぼ同一にすることができる。

【０２１４】（機器認証管理システム及び機器認証方法による作用及び効果）このような本実施形態に係る機器認証管理システム及び機器認証管理方法によれば、選定部１５ｃは、時間付加１７で付加された時間（認証管理手段から第二認証情報を取得した時間）に基づいて、その時間に対応する第二認証情報を選ぶことができるので、第二認証情報の識別子有効期限情報だけでなく、前記時間を用いることによっても第二認証情報を選ぶことができる。このため、各機器は、各機器間で有する第二認証情報がある時点で異なる場合であっても、第二認証情報の時間情報に基づいて各機器に共通する認証情報を選ぶことができる。

【０２１５】この実施形態により、各機器は、通信開始時に識別子情報をやりとりする必要がないため、例えば８０２．１１のような、通信の受信者数が複数ある場合（不特定多数である場合）でも認証情報を選ぶ手段を得られる。

【０２１６】

【発明の効果】以上説明したように本発明の機器認証管理システム及び機器認証管理方法によれば、各機器１０が、他の機器１０が有する第二認証情報に含まれる識別子を取得し、その取得した識別子と、取得情報蓄積部１２に蓄積されている第二認証情報に含まれる識別子との間で共通する前記識別子を抽出して、その抽出した識別子に対応する有効期限情報に基づいて該有効期限情報に対応する一つの第二認証情報を選定することができるので、各機器は、現時点において各機器に有する認証情報が同一でなくても（認証情報の有効期限の終了時期が異なる場合でも）、各機器に有する複数の認証情報のうち、各機器間に共通するいずれかの認証情報があれば、他の機器との間で通信を行うための認証を行うことができる。

【図面の簡単な説明】

【図１】本発明の第一実施形態に係る機器認証管理システムの概略構成を示すブ概略図である。

【図２】本発明の第一実施形態に係る機器認証管理システムの内部構成を示すブロック図である。

【図３】本発明の第一実施形態における認証部のＯＳＩ

40

構造を示したものである。

【図４】本発明の第一実施形態における機器が認証管理部から共通鍵を取得するまでの概念図（１）を示したものである。

【図５】本発明の第一実施形態における機器が認証管理部から共通鍵を取得するまでの概念図（２）を示したものである。

【図６】本発明の第一実施形態における機器が認証管理部から共通鍵を取得するまでの概念図（３）を示したものである。

【図７】本発明の第一実施形態における認証管理部が複数の通信方式を採用した機器を管理していることを示した図である。

【図８】本発明の第一実施形態における機器の状態遷移を示した図である。

【図９】本発明の第一実施形態における機器が認証管理部から共通鍵を取得するまでのフローを示した図である。

【図１０】本発明の第一実施形態における認証管理部が機器の登録情報を削除するまでのフローを示した図である。

【図１１】本発明の第一実施形態における機器が複数ある共通鍵のいずれかを用いて他の機器との間の認証を行うことを示した図である。

【図１２】本発明の第一実施形態における機器が他の機器間で共通鍵を用いて認証が行われるまでのフローを示したものである。

【図１３】本発明の第一実施形態における一つの機器が他の複数ある機器との間で認証を行うことを示した図である。

【図１４】本発明の第一実施形態における複数の機器が複数の共通鍵のいずれかを用いて認証を行うことを示した図である。

【図１５】本発明の第一実施形態における機器が認証管理部から共通鍵の更新を受けたときに他の機器間で行われる認証を示した図である。

【図１６】本発明の第一実施形態における機器が他の機器との間で行われている通信を行うまでのフローを示した図である。

【図１７】本発明の第一実施形態における機器が認証管理部から共通鍵を更新したときに他の機器との間で通信を行うまでのフローを示した図である。

【図１８】本発明の第一実施形態における機器が認証管理部から共通鍵を更新するまでのフローを示した図である。

【図１９】本発明の第二実施形態に係る機器認証管理システムの内部構造を示した図である。

【図２０】本発明の第二実施形態における機器が認証管理部から所定のタイミングで共通鍵を取得していることを示した図である。

41

【図２１】本発明の第二実施形態における複数の機器が認証管理部から共通鍵を所定のタイミングで取得していることを示した図（１）である。

【図２２】本発明の第二実施形態における複数の機器が認証管理部から共通鍵を所定のタイミングで取得していることを示した図（２）である。

【図２３】本発明の第二実施形態における異なる通信方式を採用した複数の機器が認証管理部から共通鍵を所定のタイミングで取得していることを示した図である。

【図２４】本発明の第二実施形態における異なる通信方式を採用した複数の機器がそれぞれ異なる更新期間で認

42

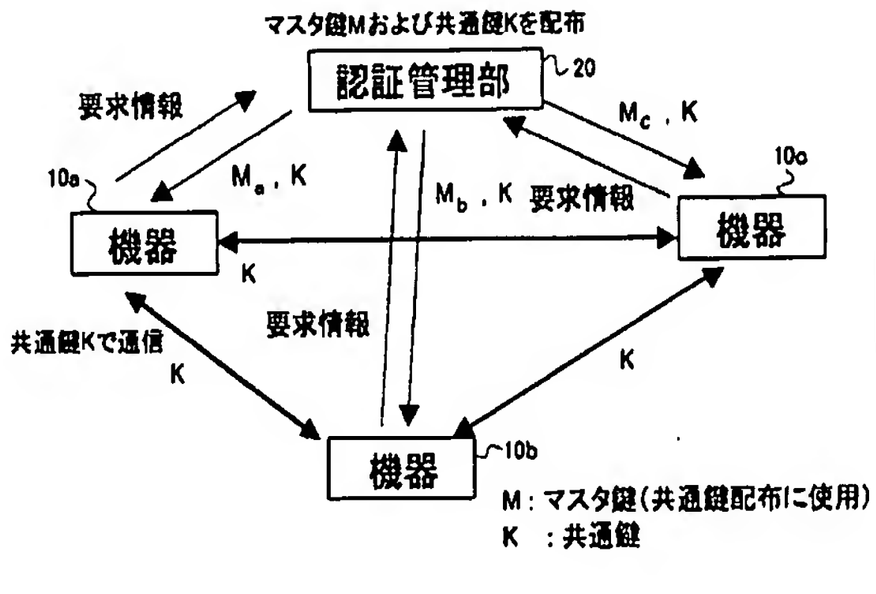
証管理部から共通鍵を取得したことを示した図である。

【図２５】従来における家庭内無線ネットワークを示した図である。

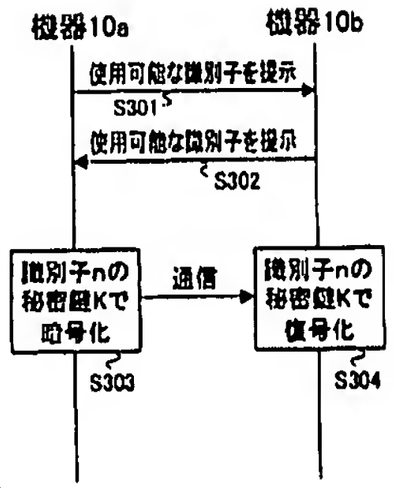
【符号の説明】

１０…機器、１１…操作部、１２…取得情報蓄積部、１３…取得情報管理部、１４…通信部、１５…認証情報決定部、１５ａ…有効期限判断部、１５ｂ…順序部、１５ｃ…選定部、１６…認証部、２０…認証管理部、２１…操作部、２２…秘密情報生成部、２３…秘密情報蓄積部、２４…秘密情報管理部、２５…通信部、２６…認証部

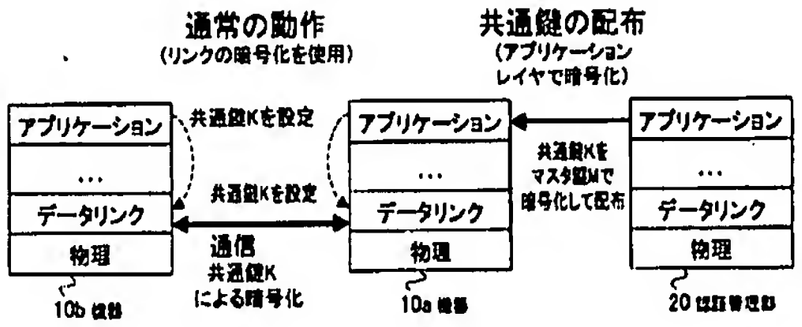
【図１】



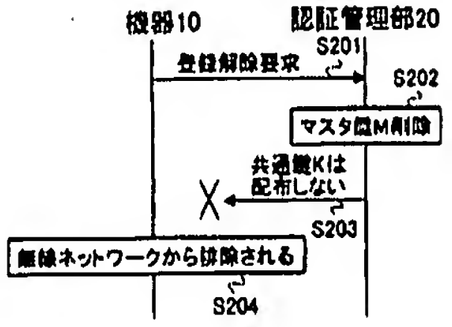
【図１２】



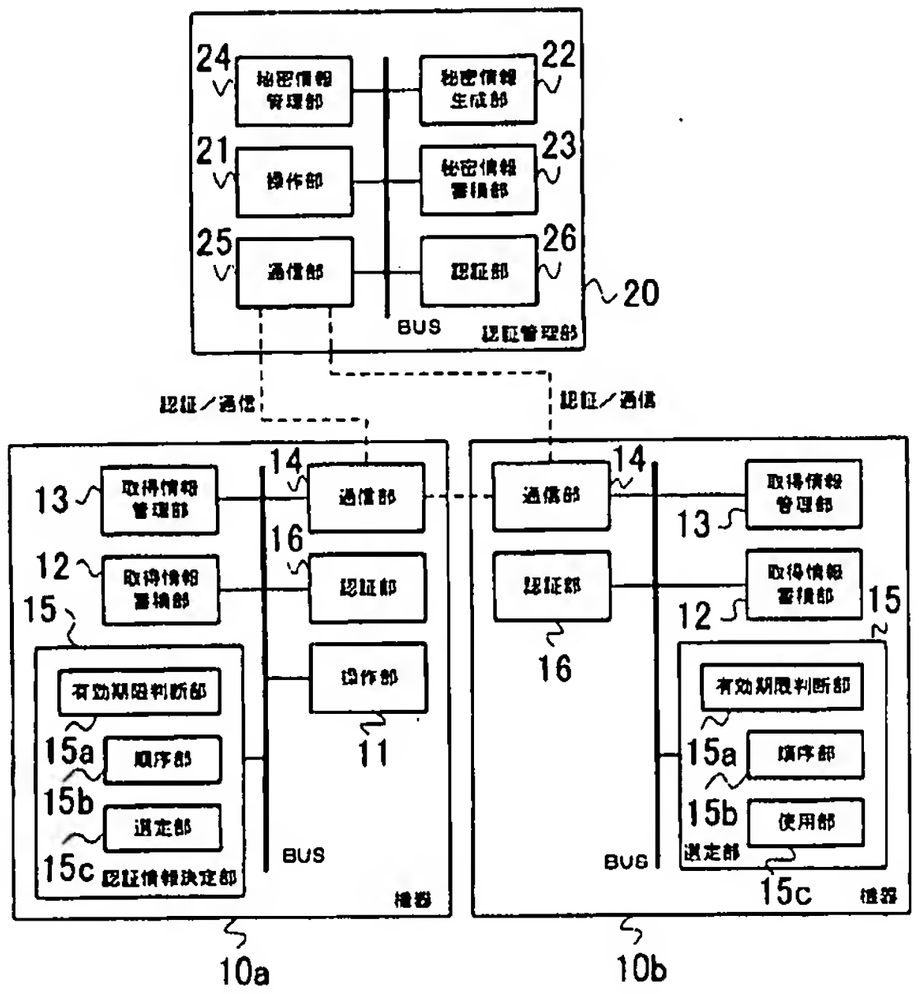
【図３】



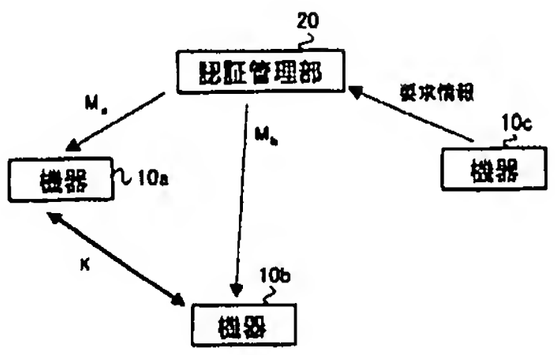
【図１０】



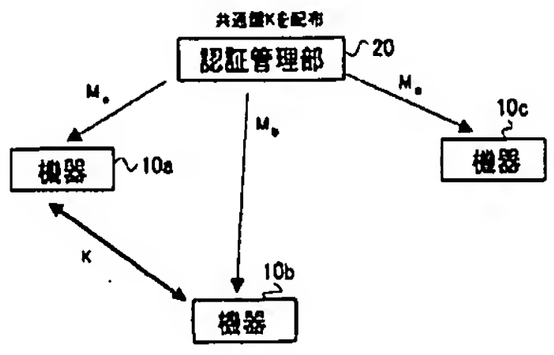
【図２】



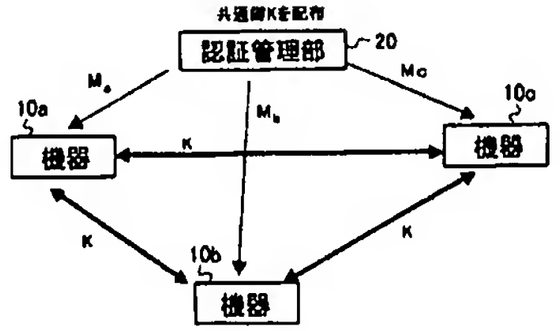
【図４】



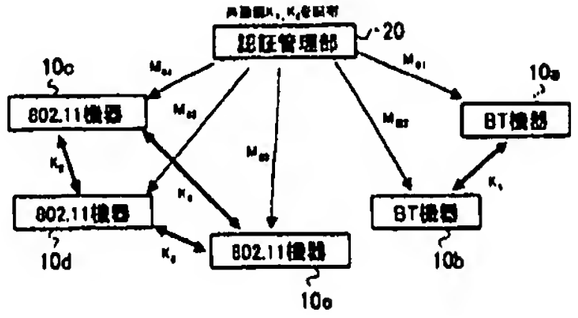
【図５】



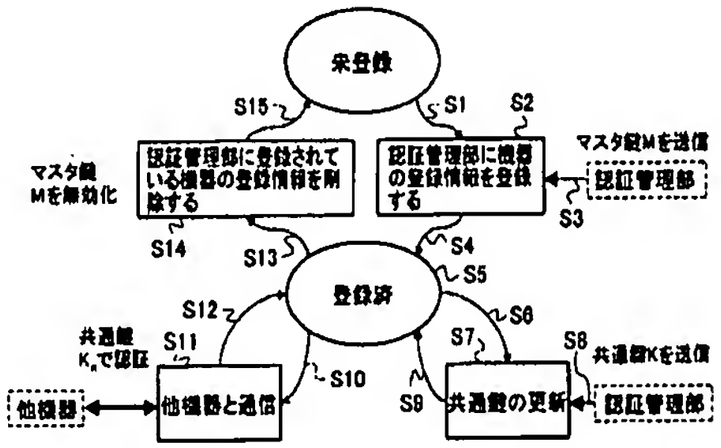
【図６】



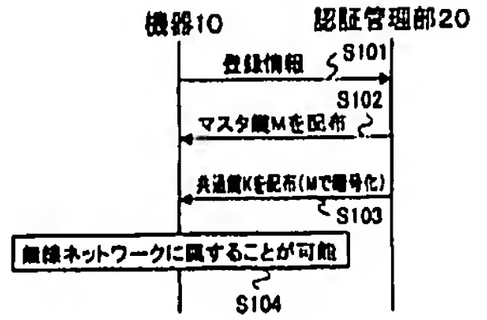
【図７】



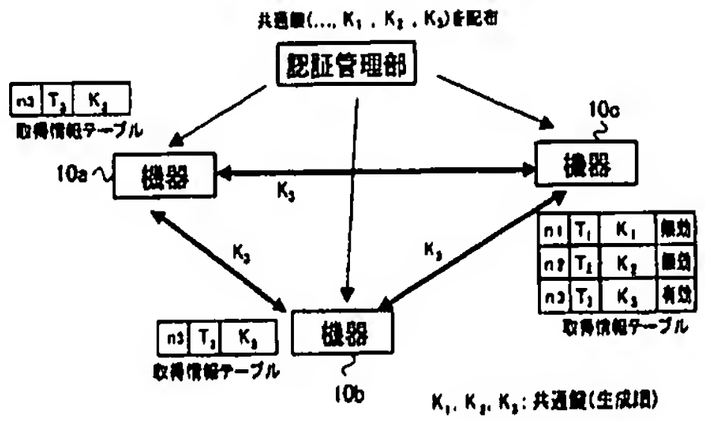
【図８】



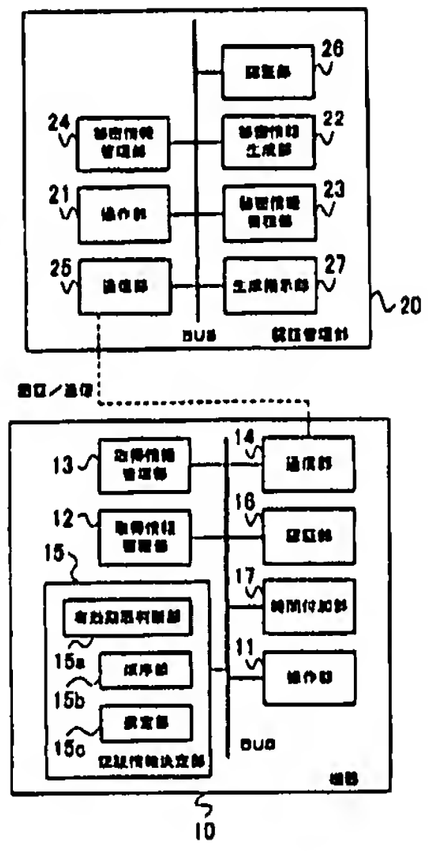
【図９】



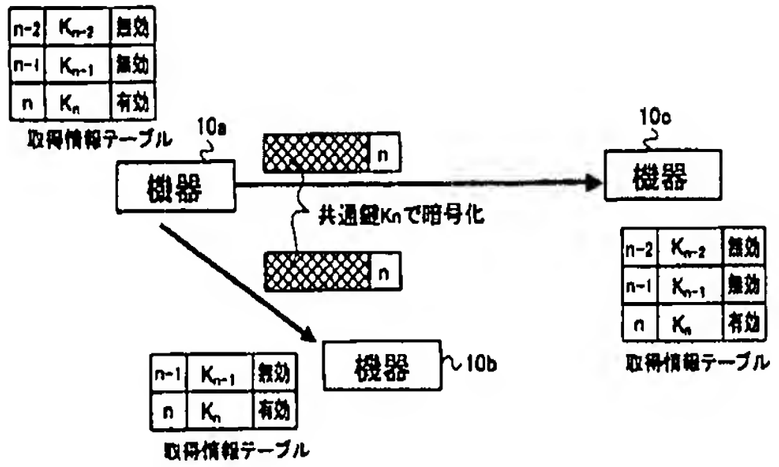
【図１１】



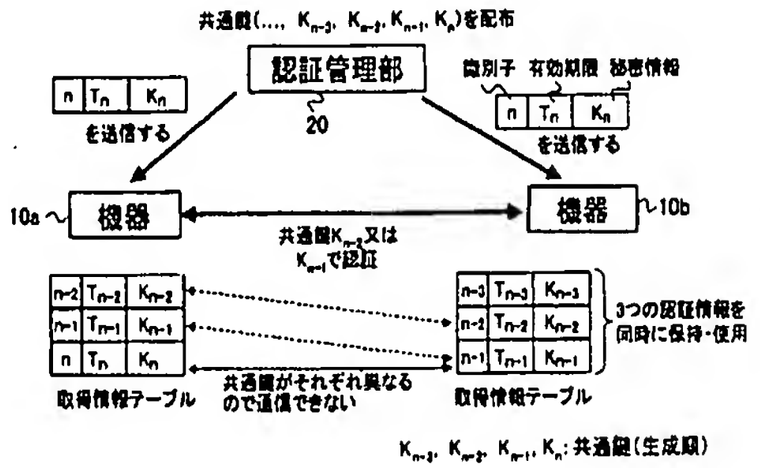
【図１９】



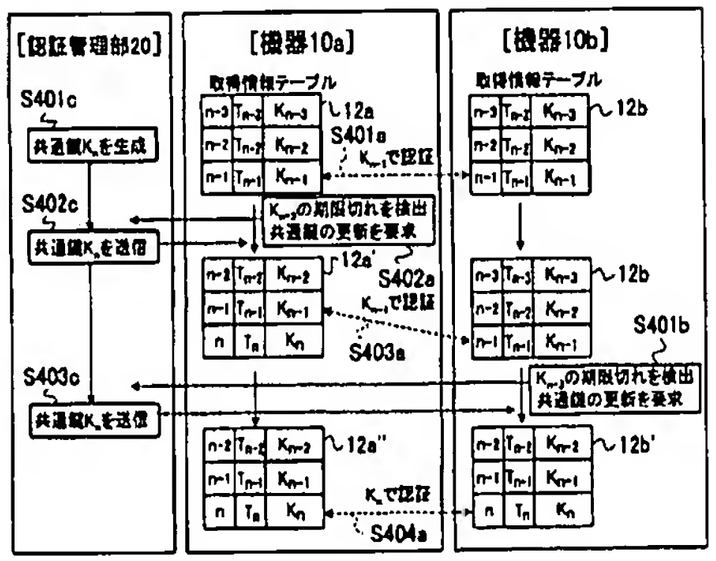
【図１３】



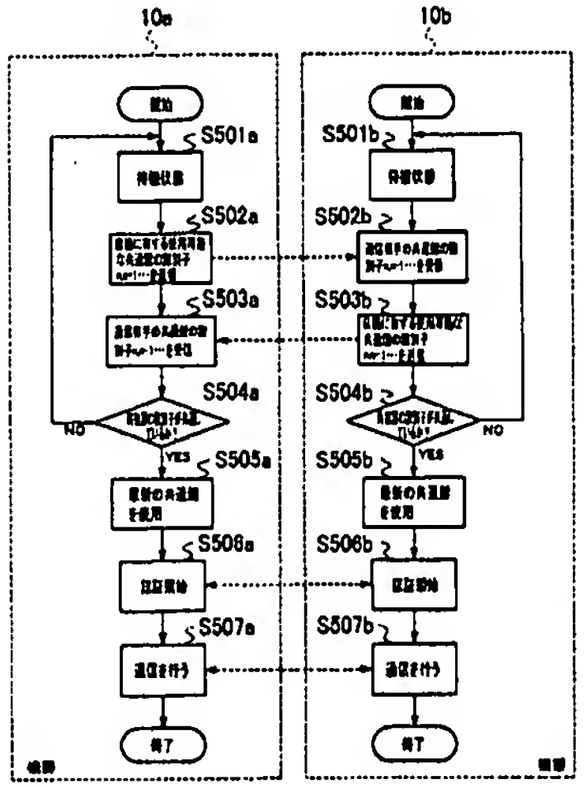
【図１４】



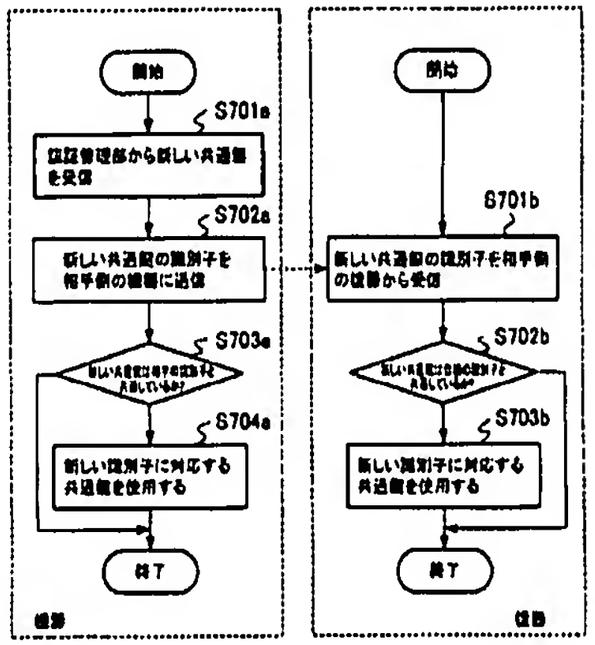
【図１５】



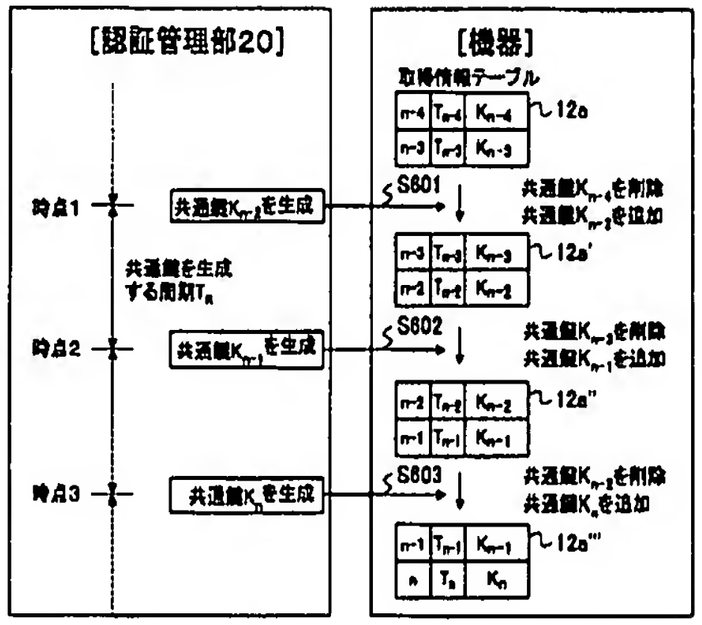
【図１６】



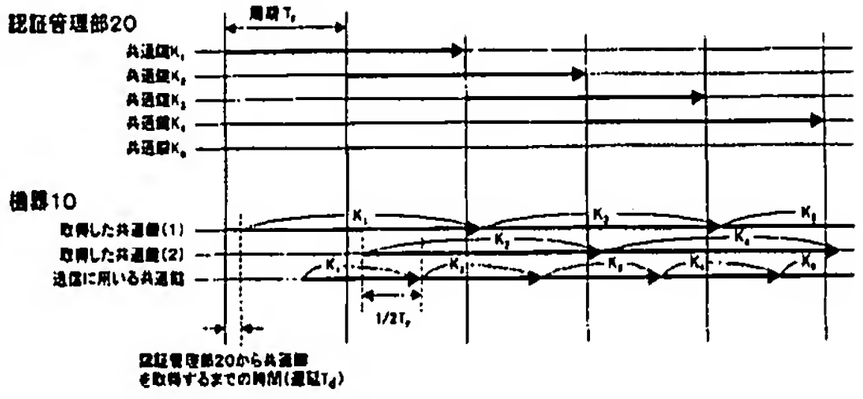
【図１７】



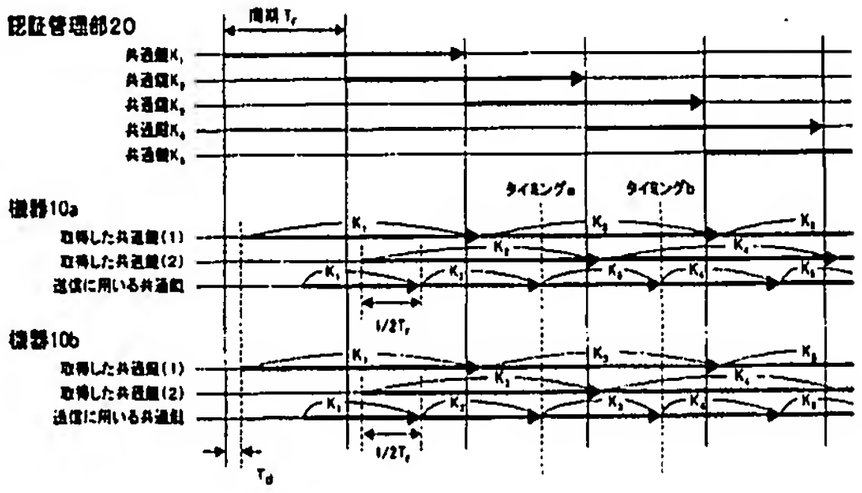
【図１８】



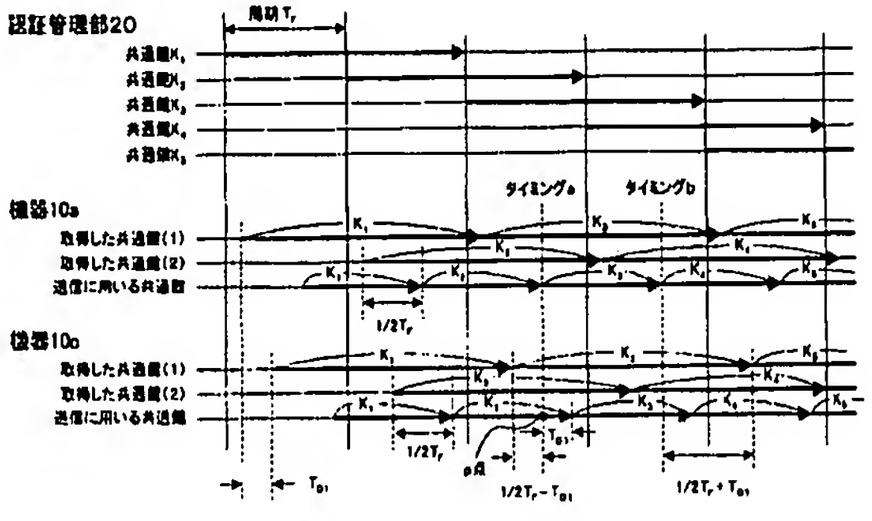
【図２０】



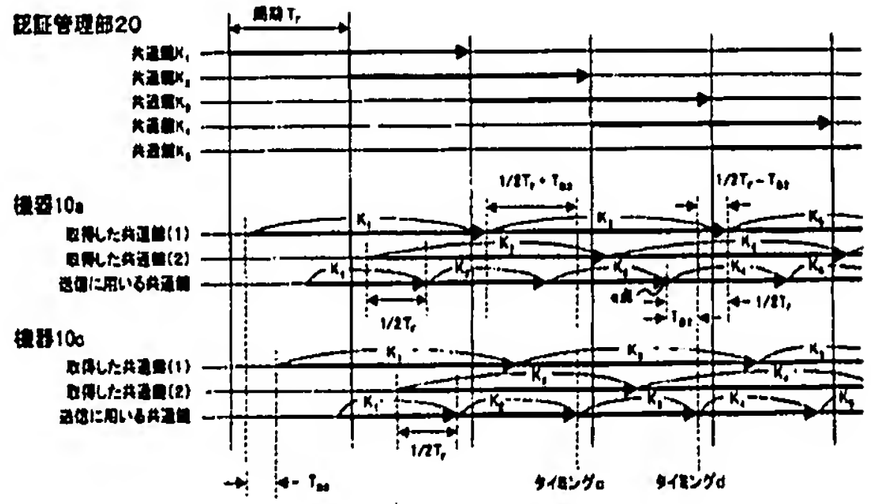
【図２１】



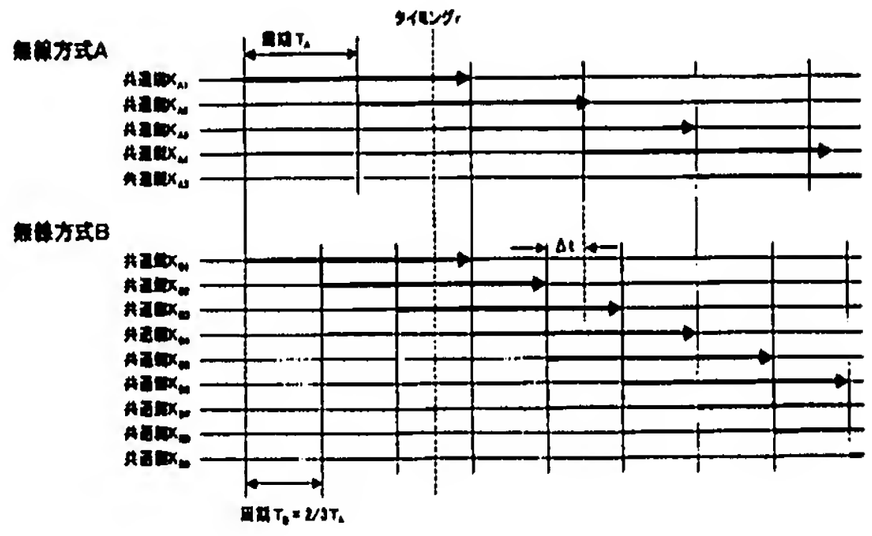
【図２２】



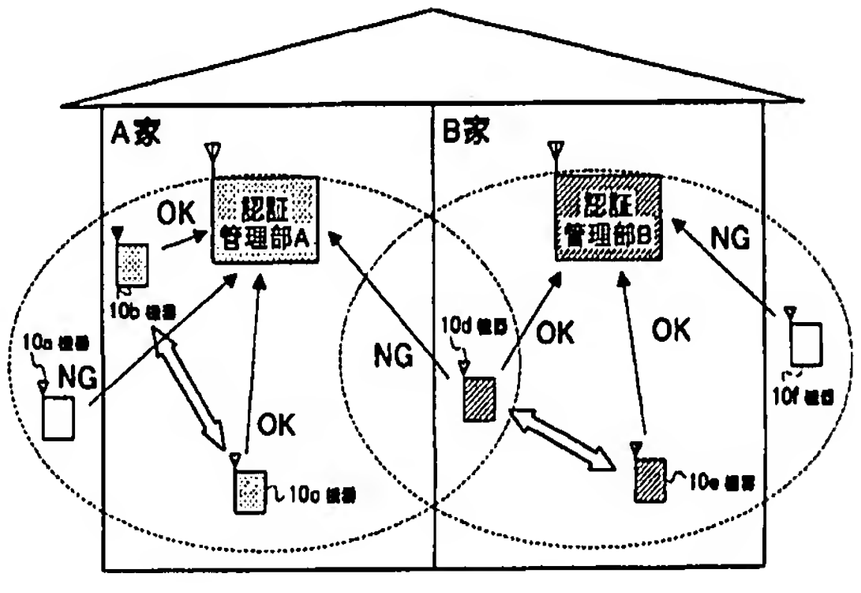
【図２３】



【図２４】



【図２５】



フロントページの続き

(72)発明者　橋本　幹生
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

Ｆターム(参考)　5B085 AE13 AE23
5J104 AA07 AA16 EA06 EA18 KA02 KA04 KA09 MA01 NA02